Payment Card Industry
Estándar de Seguridad de Datos

Requisitos y Procedimientos de Evaluación

Versión 4.0

Marzo de 2022

Cambios en el Documento

Fecha	Versión	Descripción
Octubre de 2008	1.2	Para introducir PCI DSS v1.2 como “Procedimientos de Evaluación de Seguridad y Requisitos de PCI DSS”, eliminando la redundancia entre documentos y realizando cambios tanto generales como específicos de los Procedimientos de Auditoría de Seguridad PCI DSS v1.1. Para obtener información completa, consulte el Resumen de Cambios del Estándar de Seguridad de Datos PCI de la versión 1.1 a 1.2 PCI DSS.
Julio de 2009	1.2.1	Agregue la oración que se eliminó incorrectamente entre PCI DSS v1.1 y v1.2.
		Corrija "entonces" por "que" en los procedimientos de prueba 6.3.7.a y 6.3.7.b.
		Elimine las marcas en gris en las columnas "en el lugar" y "no en lugar" en el procedimiento de prueba 6.5.b.
		Para la Hoja de Trabajo de Controles compensatorios - Ejemplo Completo, corrija la redacción en la parte superior de la página para indicar, "Utilice esta hoja de trabajo para definir controles compensatorios para cualquier requisito anotado como" en lugar " a través de Controles Compensatorios".
Octubre de 2010	2.0	Actualización y cambios implementados desde v1.2.1. Referirse a PCI DSS – Resumen de Cambios de la Versión PCI DSS 1.2.1 a 2.0.
Noviembre de 2013	3.0	Actualización desde v2.0. Referirse a PCI DSS –Resumen de Cambios de la Versión PCI DSS 2.0 a 3.0.
Abril de 2015	3.1	Actualización PCI DSS v3.0. Referirse a PCI DSS – Resumen de Cambios de la Versión 3.0 a 3.1 para ver los cambios en detalle.
Abril de 2016	3.2	Actualización de PCI DSS v3.1. Referirse a PCI DSS – Resumen de Cambios de la Versión PCI DSS 3.1 a 3.2 para ver los cambios en detalle.
Mayo de 2018	3.2.1	Actualización de PCI DSS v3.2. Referirse a PCI DSS – Resumen de Cambios de la Versión PCI DSS 3.2 a 3.2.1 para ver los cambios en detalle.
Marzo de 2022	4.0	Cambiar el nombre del título del documento a “Payment Card Industry Estándar de Seguridad de Datos: Requisitos y Procedimientos de Evaluación de Seguridad.” Actualización PCI DSS v3.2.1. Ver PCI DSS – Resumen de Cambios PCI DSS Versión 3.2.1 a 4.0 para detalles de los cambios.

DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerar se, 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.

Tabla de Contenido

1 Introducción y Visión General del Estándar de Seguridad de Datos PCI

El Estándar de Seguridad de Datos de Payment Card Industry (PCI DSS) se desarrolló para fomentar y mejorar la seguridad de los datos del tarjetahabiente y para facilitar la adopción generalizada de medidas de seguridad de datos consistentes a nivel mundial. PCI DSS proporciona una base de requisitos técnicos y operativos diseñados para proteger los datos del tarjetahabiente. Si bien está diseñado específicamente para enfocarse en entornos con datos de cuentas de tarjetas de pago, PCI DSS también se pueden utilizar para proteger de amenazas y asegurar otros elementos en el ecosistema de pagos.

La Tabla 1 muestra los 12 requisitos principales PCI DSS.

Tabla 1. Requisitos Principales PCI DSS

Estándar de Seguridad de Datos PCI: Descripción General de Alto Nivel	
Construir y Mantener Redes y Sistemas Protegidos	**1.** Instalar y Mantener los Controles de Seguridad de la Red. **2.** Aplicar Configuraciones Seguras a Todos los Componentes del Sistema.
Proteger los Datos del Tarjetahabiente	**3.** Proteger los Datos de Tarjetahabientes Almacenados. **4.** Proteger los Datos de Tarjetahabientes con Criptografía Robusta Durante la Transmisión a través de Redes Abiertas y Públicas.
Mantener un Programa de Gestión de Vulnerabilidades	**5.** Proteger Todos los Sistemas y Redes de Software Malicioso. **6.** Desarrollar y Mantener Sistemas y Softwares Seguros.
Implementar Medidas Sólidas de Control de Acceso	**7.** Restringir el Acceso a los Componentes del Sistema y a los Datos de Tarjetahabientes Según la Necesidad de Conocimiento de la Empresa. **8.** Identificar a los Usuarios y Autenticar el Acceso a los Componentes del Sistema **9.** Restringir el Acceso Físico a los Datos de Tarjetahabientes.
Monitorear y Verificar las Redes Regularmente	**10.** Registrar y Supervisar Todos los Accesos a los Componentes del Sistema y a los Datos de Tarjetahabientes. **11.** Poner a Prueba Regularmente la Seguridad de los Sistemas y de las Redes.
Mantener una Política de Protección Informática	**12.** Respaldar la Seguridad de la Información con Políticas y Programas Organizacionales.

Este documento, Requisitos y Procedimientos de Evaluación del Estándar de Seguridad de Datos PCI, consiste de 12 requisitos principales PCI DSS, requisitos de seguridad detallados, los procedimientos de prueba correspondiente y otra información pertinente a cada requisito. Las siguientes secciones proporcionan pautas detalladas y mejores prácticas para ayudar a las entidades a prepararse, realizar e informar acerca de los resultados de una evaluación PCI DSS. Los requisitos y procedimientos de prueba PCI DSS comienzan en la página 41.

PCI DSS involucran un conjunto mínimo de requisitos para proteger los datos de la cuenta y puede mejorarse mediante controles y prácticas adicionales para mitigar aún más los riesgos e incorporar leyes y regulaciones locales, regionales y sectoriales. Además, la legislación o los requisitos reglamentarios pueden requerir una protección específica de la información personal u otros elementos de los datos (por ejemplo, el nombre del titular de la tarjeta).

Limitaciones

Si alguno de los requisitos contenidos en este estándar entra en conflicto con las leyes locales, estatales o nacionales, se aplicarán las leyes locales, estatales o nacionales.

Recursos PCI DSS

El portal del PCI Security Standard Council (PCI SSC) (www.pcisecuritystandards.org) proporciona los siguientes recursos adicionales para ayudar a las organizaciones con sus evaluaciones y validaciones PCI DSS:

- Biblioteca de documentos, que incluye:
  - Resumen de cambios PCI DSS
  - Guía Rápida de Referencia PCI DSS
  - Directrices e Información Complementaria
  - Enfoque priorizado para PCI DSS
  - Plantilla e instrucciones para el Reporte de Cumplimiento (*Report of Compliance* o *ROC*). Guía e instrucciones para los Cuestionarios de Autoevaluación (*Self-Assessment Questionnaires o SAQ*)
  - Certificación de Cumplimiento *(Attestation of Compliance o AOC*)
- Preguntas Frecuentes (*Frequently Asked Questions o FAQ*)
- Sitio web PCI SSC para Pequeños Comerciantes.
- Cursos de Formación PCI y Seminarios Web Informativos
- *Qualified Security Assessor" o QSA,* por sus siglas en inglés y *"Approved Scanning Vendor" o ASV,* por sus siglas en inglés
- Listados de dispositivos, aplicaciones y soluciones aprobadas por PCI SSC.

El portal PCI SCC contiene más de 60 documentos e información suplementaria disponible con guías y consideraciones específicas para PCI DSS. Ejemplos incluyen:

- Asesoramiento para la Segmentación de Red y el Alcance PCI DSS
- Directrices de Computación en la Nube PCI SCC
- *"Multi-Factor Authentication" o MFA,* por sus siglas en inglés.
- Garantía de Seguridad de Terceros
- Monitoreo Eficiente de Registros Diarios.
- Guía de Pruebas de Penetración
- Mejores Prácticas para la Implementación de un Programa de Concientización sobre la Seguridad.
- Mejores Prácticas para Mantener el Cumplimiento PCI DSS
- PCI DSS para Grandes Organizaciones
- Uso de SSL /TLS Inicial e Impacto en los Análisis ASV. Uso de SSL/TLS Inicial para Conexiones de Terminales *Punto de Interacción - Punto de Venta ("Point of Interaction- Point of Sales-" o POS POI,* por sus siglas en inglés)
- Directrices de Seguridad de Productos con Token.
- Protección de Datos de Tarjetas de Pago Basadas en Teléfono

Nota: *Los documentos informativos complementan PCI DSS e identifican consideraciones y recomendaciones adicionales para cumplir con los requisitos de PCI DSS. Los documentos informativos no sustituyen, reemplazan ni amplían PCI DSS o ninguno de sus requisitos.*

Consulte la Biblioteca de Documentos en www.pcisecuritystandards.org para obtener información sobre estos y otros recursos.

Además, refiérase al Anexo G para acceder a definiciones de terminología PCI DSS.

2 Información Pertinente PCI DSS

El cumplimiento con PCI DSS es responsabilidad de todas las entidades que de alguna manera almacenan, procesan o transmiten datos de Tarjetahabientes ("*Cardholder Data"* o CHD, por sus siglas en inglés) y/o datos de autenticación sensibles *("Sensitive Authentication* Data" o SAD, por sus siglas en inglés) o que podrían impactar la seguridad del entorno de datos del Tarjetahabiente ("*Cardholder Data Environment"* o CDE, por sus siglas en inglés). Esto incluye todas las entidades que se dediquen al procesamiento de cuentas de pago con tarjetas—incluyendo comercios, procesadores, adquirentes, emisores, y otros proveedores de servicios.

Queda a discreción de las organizaciones que administran los programas de cumplimiento (como las marcas de pago y los adquirentes) determinar si alguna entidad está sujeta a cumplir o validar su cumplimiento con PCI DSS. Comuníquese con las organizaciones de interés para cualquier criterio adicional.

Definición de Datos de Cuenta, Datos de Titulares de Tarjetas y Datos Confidenciales de Autenticación

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

Tabla 2. Datos de cuenta

Datos de cuenta	
Los datos de Tarjetahabientes incluyen:	**Los datos Sensibles de Autenticación incluyen:**
• Número de cuenta principal *("Primary Account Number"* o PAN, por sus siglas en inglés) • Nombre del titular de la tarjeta • Fecha de Caducidad • Código de servicio	• Datos de pista completos (datos de banda magnética o equivalentes en un chip) • Código de Verificación de la Tarjeta • PIN / bloques de PIN

Los requisitos de PCI DSS se aplican a entidades con entornos donde los datos de la cuenta (datos del titular de la tarjeta y/o datos confidenciales de autenticación) se almacenan, procesan o transmiten, y entidades con entornos que pueden afectar la seguridad del CDE. Algunos requisitos de PCI DSS también pueden aplicarse a entidades con entornos que no almacenan, procesan ni transmiten datos de

cuentas, por ejemplo, entidades que sub-contratan operaciones de pago o la administración de su CDE[1]. Las entidades que sub-contratan sus entornos de pago u operaciones de pago a terceros siguen siendo responsables de garantizar que los datos de la cuenta estén protegidos por el tercero según los requisitos aplicables PCI DSS.

El número de cuenta principal (PAN) es el factor que define los datos del titular de la tarjeta. Por lo tanto, el término datos de la cuenta involucra lo siguiente: los datos PAN completos, cualquier otro elemento de los datos del titular de la tarjeta que estén presente en los datos PAN y cualquier elemento de los datos confidenciales de autenticación.

Si el nombre del titular de la tarjeta, el código de servicio y/o la fecha de caducidad se almacenan, procesan o transmiten con los datos PAN, o están presentes en el CDE, estos deben estar protegidos de acuerdo con los requisitos de PCI DSS aplicables a los datos del titular de la tarjeta.

Si una entidad almacena, procesa o transmite datos PAN, entonces existe un CDE al que se aplicarán los requisitos de PCI DSS. Algunos requisitos pueden no ser aplicables, por ejemplo, si la entidad no almacena datos PAN, entonces los requisitos relacionados con la protección de datos PAN almacenados bajo el Requisito 3 no serán aplicables a la entidad.

Incluso si una entidad no almacena, procesa o transmite datos PAN, es posible que se apliquen algunos requisitos de PCI DSS. Considere lo siguiente:

- Si la entidad almacena SAD, se aplicarán los requisitos específicamente relacionados con el almacenamiento de SAD en el Requisito 3.
- Si la entidad contrata a proveedores de servicios externos para almacenar, procesar o transmitir datos PAN en su nombre, se aplicarán los requisitos relacionados con la gestión de proveedores de servicios en el Requisito 12.
- En caso de que la entidad puede afectar la seguridad de un CDE, debido a que la seguridad de la infraestructura de una entidad puede afectar la forma en que se procesan los datos de los titulares de las tarjetas (por ejemplo, a través de un servidor web que controla la generación de un formulario o página de pago) se aplicarán algunos requisitos.
- Si los datos del titular de la tarjeta sólo aparecen en medios físicos (por ejemplo, papel), se aplicarán los requisitos de seguridad y disposición de los soportes físicos del requisito 9 cuando aplique.
- Los requisitos relacionados a un plan de respuesta a incidentes son aplicables a todas las entidades para garantizar que existen procedimientos a seguir en caso de que se sospeche o se produzca una violación a la confidencialidad de los datos de los titulares de las tarjetas.

[1] Según las organizaciones que administran programas de cumplimiento (como marcas de pago y adquirentes); las entidades deben comunicarse con las organizaciones interesadas para obtener más detalles.

Uso de los Datos de Cuentas, Datos Confidenciales de Autenticación, Datos del Titular de la Tarjeta y el Número de Cuenta Principal en PCI DSS

PCI DSS incluyen requisitos que se refieren específicamente a los datos de cuenta, los datos del Tarjetahabiente y los datos confidenciales de autenticación. Es importante tener en cuenta que cada uno de estos tipos de datos es diferente y los términos no son intercambiables. Existen referencias específicas dentro de los requisitos para atender particularmente los requisitos relacionados con datos de cuentas, datos de Tarjetahabientes o datos de autenticación sensibles al que hacen referencia.

Elementos de los Datos de la Cuenta y Requisitos de Almacenamiento

La Tabla 3 identifica los elementos relacionados con los datos del titular de la tarjeta y los datos confidenciales de autenticación, independiente de que permita o se prohíba el almacenamiento de algún dato, y aunque cada dato deba hacerse ilegible, como por ejemplo, mediante la criptografía sólida de datos, cuando se almacenan. Esta tabla no es exhaustiva y se presenta sólo para ilustrar cómo se aplican los requisitos establecidos a los diferentes tipos de datos.

Tabla 3. Requisitos de Almacenamiento de los Elementos de los Datos de la Cuenta

		Elementos de los Datos	Restricciones de Almacenamiento	Condiciones Requeridas para que los Datos Almacenados Sean Ilegibles
Datos de cuenta	**Datos del Titular de la Tarjeta**	Número de cuenta principal (PAN)	El Almacenamiento se reduce al mínimo, tal como se define en Requisito 3.2	Sí, como se define en el Requisito 3.5
		Nombre del titular de la tarjeta	El almacenamiento se reduce al mínimo, tal y como se define en el Requisito 3.2[2]	No
		Código de servicio		
		Fecha de Caducidad		
	Datos confidenciales de autenticación	Datos de Pista Completo	No pueden almacenarse después de la autorización como se define en el Requisito 3.3.1[3]	Sí, los datos almacenados hasta que se complete la autorización deben estar protegidos con criptografía sólida compleja como se define en el Requisito 3.3.2
		Código de Verificación de la Tarjeta		
		PIN y Bloque de PIN		

De acuerdo al Requisito 3.5.1 PCI DSS, si los datos PAN se almacenan con otros elementos de los datos del titular de la tarjeta, sólo los datos PAN deben ser ilegibles.

Los datos confidenciales de autenticación no deben almacenarse después de la autorización ni siquiera aunque estén cifrados. Esto aplica incluso a los ambientes en los que no hay presentes datos del PAN.

[2] Cuando los datos existen en el mismo entorno que los datos PAN.
[3] Salvo lo permitido para los emisores y las empresas que apoyan los servicios de emisión. Los requisitos para emisores y servicios de emisión se definen por separado en el Requisito 3.3.3.

3 Relación entre PCI DSS y los Estándares de Software PCI SCC

PCI SCC apoyan el uso de software de pago seguro dentro de los ambientes de datos de los titulares de tarjetas (CDE) a través del Estándar de Seguridad de Datos de Aplicaciones de Pago (PA-DSS) y del Marco de Software de Seguridad (SSF), que consiste en el Estándar de Software Seguro y en el Estándar del Ciclo de Vida del Software Seguro (SLC Seguro). El software validado y listado por PCI SCC proporciona la garantía de que el software ha sido desarrollado utilizando prácticas seguras y ha cumplido con un conjunto definido de requisitos de seguridad del software.

Los programas de software seguro PCI SSC incluyen listados de software de pago y de proveedores de software que han sido validados por cumplir con los estándares de software PCI SSC aplicables.

- **Software Validado**: El Software de Pago que figura en el portal PCI SCC como aplicación de pago validada (PA-DSS) o software de pago validado (el estándar de software seguro) ha sido evaluado por un asesor cualificado para confirmar que el software cumple con los requisitos de seguridad de dicha estándar. Los requisitos de seguridad de estos estándares se centran en la protección de la integridad y la confidencialidad de las operaciones de pago y de los datos del tarjetahabiente.
- **Proveedores de Software Validados**: El Estándar SLC Seguro define los requisitos de seguridad para que los proveedores de software integren prácticas de desarrollo de software seguro a lo largo de todo el ciclo de vida del software. Los proveedores de software que han sido validados para cumplir con el Estándar SLC Seguro están listados en el portal PCI SCC como Proveedores Calificados de SLC Seguro.

Nota: *La PA-DSS y el programa relacionado serán retirados en octubre de 2022. Consulte la lista PCI SCC de aplicaciones de pago validadas para conocer las fechas de caducidad de las aplicaciones validadas por la PA-DSS. Después de la fecha de caducidad, las aplicaciones aparecen como "Aceptadas Sólo para Usos Pre-existentes". Que una entidad pueda seguir utilizando una aplicación PA-DSS que haya expirado queda a discreción de las organizaciones que gestionan los programas de cumplimiento (como las marcas de pago y los adquirientes); para más detalles las entidades deben ponerse en contacto con estas organizaciones*

Para más información sobre el SSF o los PA-DSS, consulte las respectivas guías del programa en www.pcisecuritystandards.org.

Todo el software que almacena, procesa o transmite datos de cuentas, o que podría afectar la seguridad de los datos de cuentas o de un CDE, está en el ámbito de la evaluación PCI DSS de una entidad. Aunque el uso de software de pago validado respalda la seguridad del CDE de una entidad, el uso de dicho software no hace por sí mismo que una entidad cumpla con PCI DSS. La evaluación PCI DSS de la entidad debe incluir la verificación de que el software fue configurado correctamente y he e implementado de forma segura y de acuerdo con las especificaciones del proveedor y con las mismas características bajo las cuales fue certificado para apoyar los requisitos aplicables PCI DSS. Si la aplicación de pago incluida en la lista del portal PCI ha sido personalizada, será necesaria una revisión más profunda durante la evaluación PCI DSS, ya que el software puede haber dejado de ser representativo de la versión que se validó originalmente.

Dado que las amenazas a la seguridad evolucionan constantemente, es posible que el software ya no cuenta con el apoyo del proveedor como por ejemplo cuando una aplicación es identificada por el proveedor como que ha llegado a su "fin de vida" y no ofrezca el mismo nivel de seguridad que otras versiones validadas más recientemente. Se recomienda que las entidades que mantengan su software al día y actualizado con las últimas versiones de software disponibles.

Se alienta a las entidades que desarrollan su propio software a que consulten los estándares de seguridad del software PCI SCC y consideren los requisitos de las mismas como las mejores prácticas a utilizar en sus ambientes de desarrollo. Un software de pago seguro implementado en un ambiente que cumpla con PCI DSS ayudará a minimizar la posibilidad de que se produzcan brechas de seguridad que faciliten el compromiso de los datos del tarjetahabiente y el fraude. Refiérase a Software Personalizado.

Aplicabilidad PCI DSS a los Proveedores de Softwares de Pago

PCI DSS pueden aplicarse a un proveedor de software de pago si éste es también un proveedor de servicios que almacena, procesa o transmite datos de cuentas, o si tiene acceso a los datos de cuentas de sus clientes, por ejemplo, cuando en calidad de proveedor de servicios de pago o mediante el acceso remoto a un ambiente CDE de un cliente. Entre los proveedores de software a los que pueden aplicarse lo PCI DSS se encuentran los que ofrecen servicios de pago, así como los proveedores de servicios en la nube que ofrecen terminales de pago en la nube, software como servicio (SaaS), comercio electrónico en la nube y otros servicios de pago en la nube.

Software A Medida y Personalizado

Todo el software a medida y personalizado que almacena, procesa o transmite datos de cuentas, o que podría afectar la seguridad de los datos de cuentas o de un CDE, está en el ámbito de la evaluación PCI DSS de una entidad.

El software a medida y personalizado que ha sido desarrollado y mantenido de acuerdo con uno de los estándares del Marco de Seguridad del Software PCI SCC (El Estándar de Software Seguro o el Estándar de SLC Seguro) servirá de apoyo a una entidad en el cumplimiento del Requisito 6 PCI DSS.

Refiérase al Anexo F para más detalles.

Nota: *El Requisito 6 PCI DSS se aplica totalmente al software personalizado que no ha sido desarrollado e implementado de acuerdo con una de los estándares del Marco de Seguridad del Software PCI SCC. Las entidades que utilicen proveedores de software para desarrollar software personalizado que pudiese afectar la seguridad de los datos del tarjetahabiente o del CDE son responsables de garantizar que sus proveedores de software desarrollen el software de forma segura y de acuerdo con lo estipulado el Requisito 6 PCI DSS.*

4 Alcance de los Requisitos de PCI DSS

Los requisitos de PCI DSS se aplican a:

- El entorno de datos del titular de la tarjeta (CDE), que se compone de:
  - Componentes del sistema, personas y procesos que almacenan, procesan y transmiten datos del titular de la tarjeta y/o datos confidenciales de autenticación, y,
  - Componentes del sistema que aunque no almacenan, procesan o transmiten CHD/SAD pero que tienen una conectividad sin restricciones con componentes del sistema que almacenan, procesan o transmiten CHD/SAD.

Y

- Componentes del sistema, personas y procesos que podrían afectar la seguridad del CDE.[4]

"Los componentes del sistema" incluyen dispositivos de red, servidores, de computación computadoras personales y portátiles, componentes virtuales, componentes en la nube y software. Los ejemplos de componentes del sistema incluyen, pero no se limitan a:

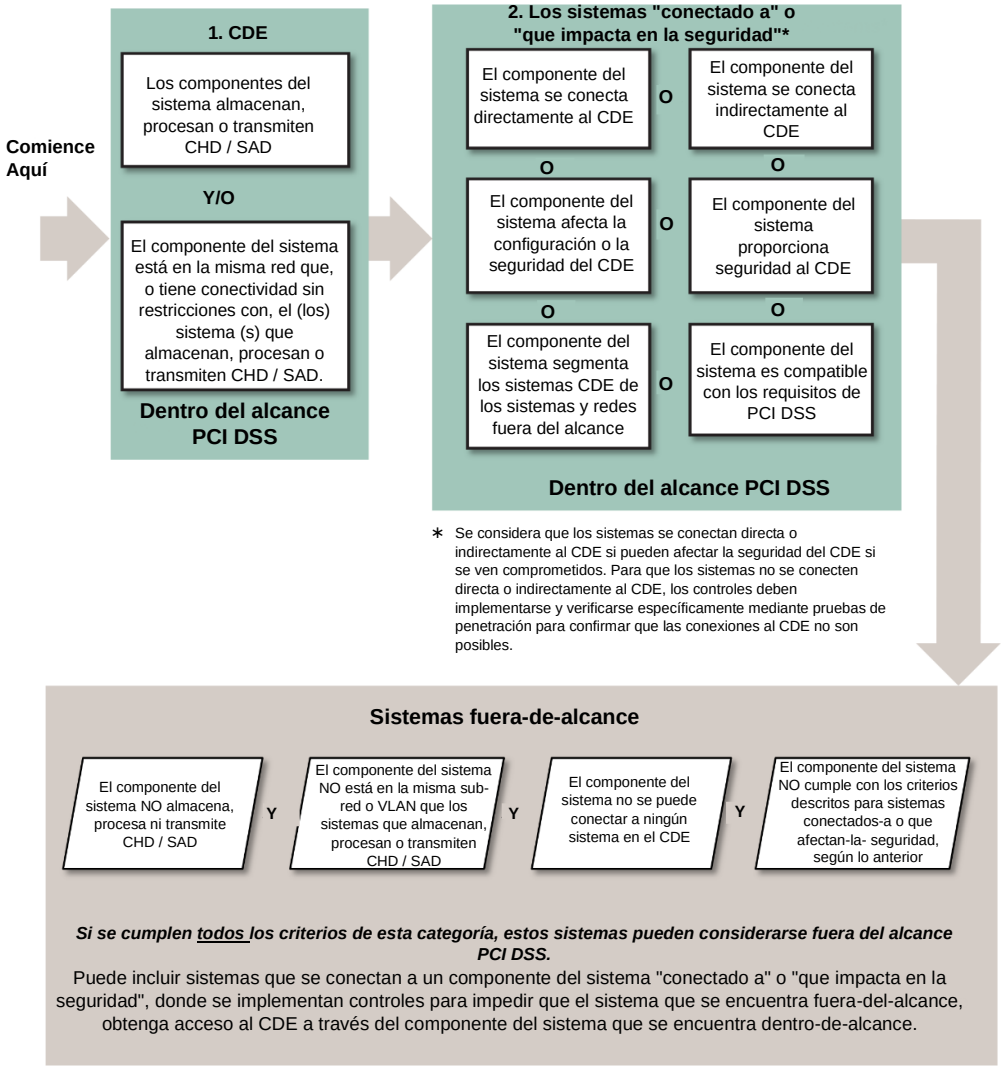
- Sistemas que almacenan, procesan o transmiten datos de cuentas como por ejemplo, terminales de pago, sistemas de autorización, sistemas de compensación, sistemas *middleware* de pago, sistemas de *back-office* de pago, sistemas de carros de compra y frontales de tiendas, sistemas de pasarela de pagos, sistemas de monitoreo de fraude).
- Sistemas que prestan servicios de seguridad como por ejemplo, servidores de autenticación, servidores de control de acceso, sistemas para incidentes y la correlación de eventos e incidentes de seguridad (SIEM) y sistemas de seguridad física como por ejemplo, acceso con tarjeta de identificación o sistemas de video vigilancia (CCTV), sistemas de Autenticación Multi-Factor (MFA) y sistemas que protegen contra softwares maliciosos).
- Sistemas que facilitan la segmentación de la red y la implementación controles de seguridad en la red interna.
- Sistemas que puedan afectar la seguridad de los datos del tarjetahabiente o del CDE como por ejemplo la resolución de nombres o redirección de servidores de comercio electrónico en la *web*.
- Componentes de virtualización como por ejemplo máquinas virtuales," *switches/routers"* virtuales, "*appliances"* virtuales, aplicaciones /"desktop" virtuales y hipervisores.
- Infraestructura y componentes en la nube, tanto externos como en sitio, e incluyendo instancia o imágenes de contenedores o imágenes, nubes privadas virtuales, manejo de identidad y control de accesos basados en la nube, CDE residiendo en sitio o en la nube, servicios de "meses" aplicaciones en contenedores, y herramientas de orquestación de contenedores.

[4] Para orientación adicional, consulte el *Documento de información: Asesoramiento para el alcance y la Segmentación de Red* PCI DSS en el sitio web PCI SCC.

- Componentes de red, incluidos, entre otros, los controles de seguridad de la red, "firewalls*", "switches", "routers",* dispositivos VoIP, puntos de acceso inalámbricos, "*appliances"* de la red y otros dispositivos de seguridad.
- Tipos de servidores, incluidos, entre otros, los de web, aplicaciones, bases de datos, autenticación, correo, proxy, Protocolo Tiempo en la Red (NTP) y de Nombre de Dominio (DNS).
- Dispositivos para usuarios, computadoras personales, computadoras portátiles, estaciones de trabajo, tabletas y dispositivos móviles.
- Impresoras y dispositivos multifunción que se utilizan para escanean, imprimen y envían faxes de documentos.
- Almacenamiento de datos de cuentas en cualquier formato (por ejemplo, papel, archivos de datos, archivos de audio, imágenes y grabaciones de vídeo).
- Aplicaciones, software y componentes de software, aplicaciones sin servidor, incluidas todas las compradas como las que son por suscripción como por ejemplo, software como servicio), softwares personalizado, incluyendo las aplicaciones internas como las y externas que se acceden por Internet).
- Herramientas, repositorios de código y sistemas para el manejo e implementación de la configuración de software o para el despliegue de objetos al CDE o a sistemas que pueden impactar el CDE.

La Figura 1 muestra las consideraciones para determinar el alcance de los componentes del sistema para PCI DSS.

Figura 1. Comprensión del alcance PCI DSS



Confirmación anual del alcance PCI DSS

El primer paso para prepararse para una evaluación PCI DSS es que la entidad determine con precisión el alcance de la revisión. La entidad evaluada debe confirmar la precisión de su alcance a PCI DSS de acuerdo con el Requisito 12.5.2 PCI DSS identificando todas las ubicaciones y flujos de datos de la cuenta e identificando todos los sistemas que están conectados o, si están comprometidos, podrían afectar el CDE (por ejemplo, servidores de autenticación, servidores de acceso remoto, servidores de registro) para garantizar que estén incluidos en el alcance PCI DSS. Se deben considerar todos los tipos de sistemas y ubicaciones durante el proceso de determinación del alcance, incluidos los sitios de apoyo/recuperación y los sistemas de conmutación por error.

Los pasos mínimos para que una entidad confirme la precisión del alcance PCI DSS se especifican en el Requisito 12.5.2 PCI DSS. Se espera que la entidad retenga documentación para mostrar cómo se determinó el alcance PCI DSS. La documentación se conserva para la revisión del asesor y como referencia durante la próxima actividad de confirmación del alcance PCI DSS de la entidad. Para cada evaluación PCI DSS, el asesor valida que la entidad definió y documentó con precisión el alcance de la evaluación.

Nota: *Esta confirmación anual del alcance PCI DSS se define en el Requisito de PCI DSS en 12.5.2 y es una actividad que se espera sea desarrollada por la entidad. Esta actividad no es la misma, ni está destinada a ser reemplazada por la confirmación del alcance realizada por el asesor de la entidad durante la evaluación.*

Segmentación

La segmentación (o aislamiento) del CDE del resto de la red de una entidad no es un requisito de PCI DSS. Sin embargo, es un método muy recomendado que puede reducir:

- Alcance de la evaluación PCI DSS
- Costo de la evaluación PCI DSS
- Costo y dificultad de implementar y mantener controles PCI DSS
- Riesgo para una organización en relación con los datos de la cuenta de la tarjeta de pago (se reduce al consolidar esos datos en menos ubicaciones más controladas)

Sin una segmentación adecuada (a veces denominada "red plana"), toda la red está dentro del alcance de la evaluación PCI DSS. La segmentación se puede lograr utilizando varios métodos físicos o lógicos, como controles de seguridad de red internos configurados correctamente, enrutadores con listas de control de acceso sólidos u otras tecnologías que restringen el acceso a un segmento particular de una red. Para que se considere fuera del alcance PCI DSS, el componente del sistema debe estar segmentado (aislado) correctamente del CDE, de forma tal que el componente del sistema que está fuera de alcance no pueda afectar la seguridad del CDE, incluso si ese componente se vio comprometido.

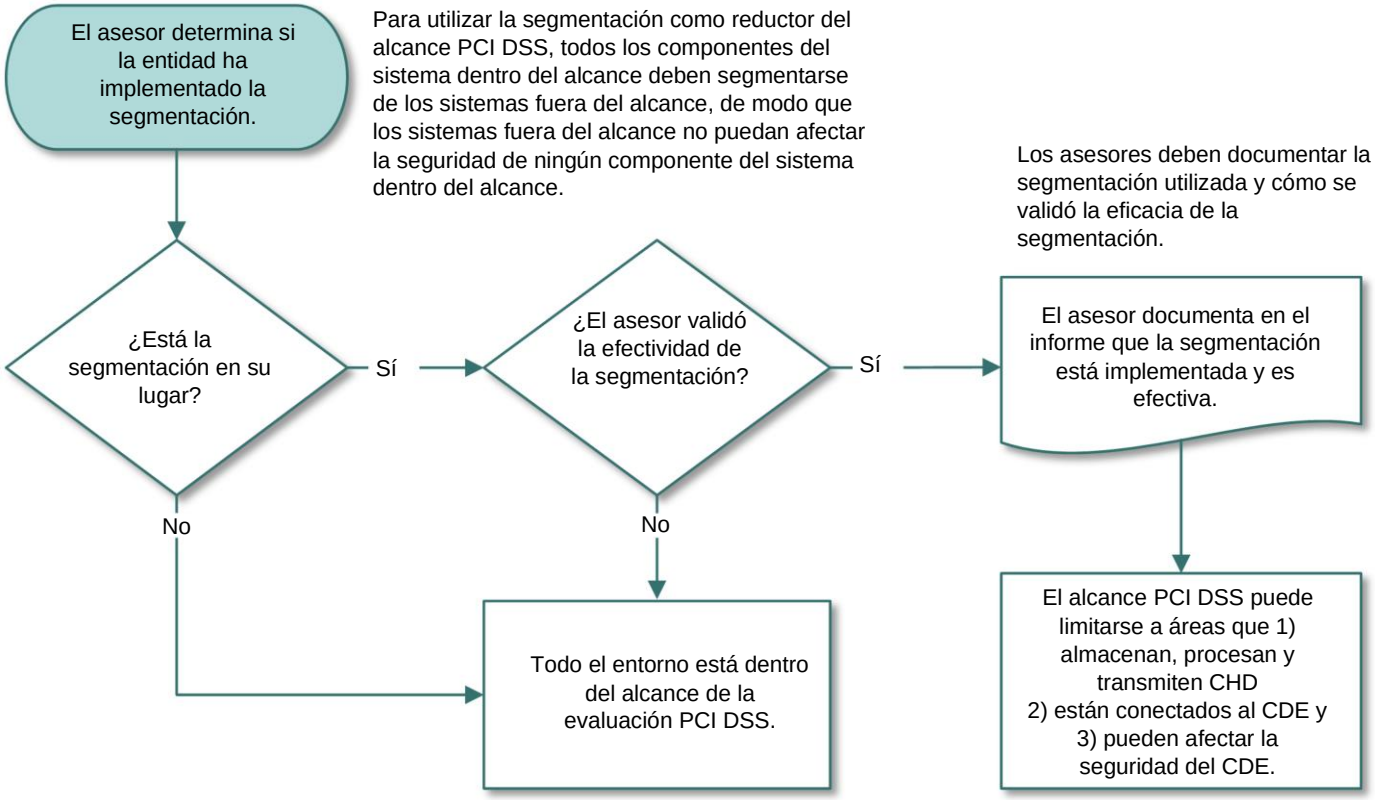
Un requisito previo importante para reducir el alcance del CDE es una comprensión clara de las necesidades y los procesos de negocios relacionados con el almacenamiento, el procesamiento y la transmisión de los datos de la cuenta. Restringir los datos de la cuenta a la menor

cantidad posible de ubicaciones mediante la eliminación de datos innecesarios y la consolidación de los datos necesarios puede requerir la re-ingeniería de prácticas de negocios tradicionales.

Documentar los flujos de datos de la cuenta a través de un diagrama de flujo de datos ayuda a la entidad a entender ampliamente cómo los datos de la cuenta ingresan a una organización, dónde residen dentro de la organización y cómo atraviesan varios sistemas dentro de la organización. Los diagramas de flujo-de datos también ilustran todas las ubicaciones donde se almacenan, procesan y transmiten los datos de la cuenta. Esta información respalda a una entidad que implementa la segmentación y también puede respaldar la confirmación de que la segmentación se está utilizando para aislar el CDE de las redes fuera de alcance.

Si la segmentación se utiliza para reducir el alcance de la evaluación PCI DSS, el asesor debe verificar que la segmentación sea adecuada para reducir el alcance de la evaluación, como se ilustra en la Figura 2. En niveles elevados, la segmentación adecuada aísla los sistemas que almacenan, procesan o transmiten datos de cuentas de aquellos que no lo hacen. Sin embargo, la conveniencia de la implementación de una segmentación específica es muy variable y depende de varios factores, como la configuración de una red determinada, las tecnologías implementadas y otros controles que puedan implementarse.

Figura 2. Segmentación e impacto en el alcance PCI DSS



Inalámbrico

Si se utiliza tecnología inalámbrica para almacenar, procesar o transmitir datos de la cuenta (por ejemplo, dispositivos inalámbricos de punto de venta), o si una red de área local inalámbrica (WLAN) forma parte o está conectada al CDE, los requisitos de PCI DSS y los procedimientos de prueba para proteger los entornos inalámbricos se aplican y deben llevarse a cabo.

La detección inalámbrica no autorizada debe realizarse de acuerdo con el Requisito 11.2.1 PCI DSS incluso cuando la tecnología inalámbrica no se use dentro del CDE y si la entidad cuenta con una política que prohíba el uso de tecnología inalámbrica en su entorno. Esto se debe a la facilidad con la que se puede conectar un punto de acceso inalámbrico a una red, la dificultad para detectar su presencia, y el mayor riesgo que presentan los dispositivos inalámbricos no autorizados.

Antes de que se implemente la tecnología inalámbrica, la entidad debe evaluar cuidadosamente la necesidad de la tecnología frente al riesgo. Considere implementar tecnología inalámbrica solo para la transmisión de datos no confidenciales.

Datos Cifrados del Tarjetahabiente e Impacto en el alcance PCI DSS

El cifrado de los datos del titular de la tarjeta con criptografía sólida es un método aceptable para hacer que los datos sean ilegibles de acuerdo con el Requisito 3.5 PCI DSS. Sin embargo, el cifrado por sí solo es generalmente insuficiente para dejar los datos del titular de la tarjeta fuera del alcance PCI DSS y no elimina la necesidad PCI DSS en ese entorno. El entorno de la entidad todavía está dentro del alcance PCI DSS debido a la presencia de datos de titulares de tarjetas. Por ejemplo, para un entorno de tarjeta comercial presente, existe acceso físico a las tarjetas de pago para completar una transacción y también puede haber informes en papel o recibos con datos del titular de la tarjeta. Del mismo modo, en los entornos de negocios sin tarjeta, como la venta por correo o por teléfono y el comercio electrónico, los datos de las tarjetas de pago se facilitan a través de canales que deben ser evaluados y protegidos de acuerdo con el Estándar PCI DSS.

Los siguientes están dentro del alcance PCI DSS:

- Sistemas que realizan cifrado y/o des-cifrado de datos de titulares de tarjetas y sistemas que realizan funciones administrativas esenciales,
- Datos cifrados del titular de la tarjeta que no estén aislados de los procesos de cifrado y descodificación y de gestión de claves,
- Datos cifrados del titular de la tarjeta que están presentes en un sistema o medio que también contiene la clave de descifrado,
- Datos cifrados del titular de la tarjeta que están presentes en el mismo entorno que la clave de descifrado,
- Datos cifrados del titular de la tarjeta a los que puede acceder una entidad que también tiene acceso a la clave de descifrado.

***Nota**: Una solución P2PE listada en PCI puede reducir significativamente la cantidad de requisitos de PCI DSS aplicables al entorno de datos de titulares de tarjetas de un comerciante. Sin embargo, no elimina por completo la aplicabilidad PCI DSS en el entorno comercial.*

Datos cifrados del tarjetahabiente e impacto en el alcance PCI DSS para proveedores de servicios externos

Cuando un proveedor de servicios externos (TPSP) recibe y/o almacena solo datos cifrados por otra entidad, y cuando no tiene la capacidad de descifrar los datos, el TPSP puede considerar los datos cifrados fuera del alcance si se cumple conciertas condiciones. Esto se debe a que la responsabilidad de los datos generalmente recae en la entidad, o entidades, con la capacidad de descifrar los datos o afectar la seguridad de los datos cifrados. Determinar qué parte es responsable de los controles específicos PCI DSS dependerá de varios factores, incluido quién tiene acceso a las claves de descifrado, la función que desempeña cada parte y el acuerdo entre las partes. Las responsabilidades deben estar claramente definidas y documentadas para garantizar que tanto el TPSP como la entidad que proporciona los datos cifrados comprendan qué entidad es responsable de qué controles de seguridad.

Por ejemplo, un TPSP que proporciona servicios de almacenamiento recibe y almacena datos cifrados del titular de la tarjeta proporcionados por los clientes con fines de apoyo. Este TPSP no tiene acceso a las claves de cifrado o descifrado, ni realiza ninguna gestión de claves para sus clientes. El TPSP puede excluir dichos datos cifrados al determinar su alcance PCI DSS. Sin embargo, el TPSP mantiene la responsabilidad de controlar el acceso al almacenamiento de datos cifrados como parte de sus acuerdos de servicio con sus clientes.

La responsabilidad de garantizar que los datos cifrados y las claves criptográficas estén protegidos de acuerdo con los requisitos aplicables PCI DSS a menudo se comparte entre entidades. En el ejemplo anterior, el cliente determina quiénes, entre su personal, están autorizados a acceder a los medios de almacenamiento, y el centro de almacenamiento es responsable de administrar los controles de acceso físico y/o lógico para garantizar que solo las personas autorizadas por el cliente tengan acceso a los medios de almacenamiento. Los requisitos específicos PCI DSS aplicables a un TPSP dependerán de los servicios prestados y del acuerdo entre las dos partes. En el ejemplo de un TPSP que proporciona servicios de almacenamiento, los controles de acceso físico y lógico proporcionados por el TPSP deberán revisarse al menos una vez al año. Esta revisión podría realizarse como parte de la evaluación PCI DSS del comerciante o, alternativamente, la revisión podría ser realizada y los controles validados por el TPSP con la evidencia apropiada proporcionada al comerciante. Para obtener información sobre "evidencias apropiadas", consulte Opciones para que los TPSP validen el cumplimiento PCI DSS para los servicios TPSP que cumplen con los requisitos de PCI DSS de los clientes.

Vemos otro ejemplo, un TPSP que recibe solo datos cifrados del titular de la tarjeta con el propósito de encaminarlos hacia otras entidades, y que no tiene acceso a los datos o claves criptográficas, puede no tener ninguna responsabilidad PCI DSS por esos datos cifrados. En este escenario, donde el TPSP no proporciona ningún servicio de seguridad o controles de acceso, se pueden considerar lo mismo que una red pública o no confiable, y sería responsabilidad de las entidades que envían/ reciben datos de la cuenta a través de la red TPSP para garantizar que se apliquen los controles PCI DSS para proteger los datos que se transmiten.

Uso de Proveedores de Servicios Externos

Una entidad (a la que se hace referencia como el "cliente" en esta sección) puede optar por utilizar un proveedor de servicios externos (TPSP) para almacenar, procesar o transmitir datos de la cuenta o para administrar los componentes del sistema dentro del alcance en nombre del cliente. El uso de un TPSP puede tener un impacto en la seguridad del CDE de un cliente.

***Nota**: El uso de un TPSP certificado PCI DSS no hace que un cliente cumpla con PCI DSS, ni elimina la responsabilidad del cliente por su propio programa de cumplimiento PCI DSS. Incluso si un cliente usa un TPSP para cumplir con todas las funciones de datos de la cuenta, ese cliente sigue siendo responsable de confirmar su propio cumplimiento según lo solicitado por las organizaciones que administran los programas de cumplimiento (por ejemplo, marcas de pago y adquirentes). Los clientes deben comunicarse con las organizaciones de interés para cualquier requisito.*

El uso de TPSP y el impacto en los clientes que cumplen con el requisito 12.8 PCI DSS

Hay muchos escenarios diferentes en los que un cliente puede utilizar uno o más TPSP para funciones dentro o relacionadas con el CDE del cliente. En todos los escenarios donde se utiliza un TPSP, el cliente debe administrar y supervisar el estado de cumplimiento PCI DSS de todos sus TPSP de acuerdo con el Requisito 12.8, incluyendo los TPSP que:

- Tienen acceso al CDE del cliente,
- Administran los componentes del sistema dentro del alcance en nombre del cliente y/o
- Pueden afectar la seguridad del CDE del cliente.

La gestión de los TPSP de acuerdo con el Requisito 12.8 incluye realizar la debida diligencia, aplicar los acuerdos adecuados en vigor, identificar qué requisitos se aplican al cliente y cuáles se aplican al TPSP, y monitorear el estado de cumplimiento de los TPSP al menos una vez al año.

El requisito 12.8 no especifica que los TPSP del cliente deben cumplir con PCI DSS, solo que el cliente supervise su estado de cumplimiento como se especifica en el requisito. Por lo tanto, los TPSP no necesitan estar certificados en PCI DSS para que su cliente cumpla con el Requisito 12.8.

Impacto del Uso de los TPSP para Servicios que Cumplen con los Requisitos de PCI DSS de los clientes

Cuando el TPSP proporciona un servicio que cumple con los requisitos de PCI DSS en nombre del cliente o cuando ese servicio puede afectar la seguridad del CDE del cliente, esos requisitos están dentro del alcance de la evaluación del cliente y el cumplimiento de ese servicio afectará el cumplimiento PCI DSS del cliente. El TPSP debe demostrar que cumple con los requisitos de PCI DSS aplicables para que esos requisitos estén vigentes para sus clientes. Por ejemplo, si una entidad contrata un TPSP para administrar sus controles de seguridad de red, y el TPSP no proporciona evidencia de que cumple con los requisitos aplicables descritos en el Requisito 1 PCI DSS, entonces esos requisitos no están vigentes para la evaluación del cliente. Como otro ejemplo, los TPSP que almacenan copias

de seguridad con los datos del titular de la tarjeta en nombre de los clientes deberían cumplir con los requisitos aplicables relacionados con los controles de acceso, la seguridad física, etc., para que sus clientes consideren esos requisitos para sus evaluaciones.

La Importancia de Comprender las Responsabilidades Entre los Clientes de TPSP y los TPSP

Los clientes y los TPSP deben identificar y comprender claramente lo siguiente:

- Los servicios y componentes del sistema incluidos en el alcance de la evaluación PCI DSS del TPSP,
- Los requisitos y sub-requisitos específicos PCI DSS cubiertos por la evaluación PCI DSS del TPSP,
- Cualquier requisito que sea responsabilidad de los clientes del TPSP para incluir en sus propias evaluaciones PCI DSS, y
- Cualquier requisito de PCI DSS cuya responsabilidad sea compartida entre el TPSP y sus clientes.

Por ejemplo, un proveedor de servicios en la nube debe definir claramente cuáles de sus direcciones IP son escaneadas como parte de su proceso de escaneo trimestral de vulnerabilidades y cuáles direcciones IP son responsabilidad de sus clientes para escanear.

Acorde al requisito 12.9.2, los TPSP deben apoyar con las solicitudes de información de sus clientes sobre el estado de cumplimiento PCI DSS por parte del TPSP en relación con los servicios prestados a los clientes, y sobre qué requisitos de PCI DSS son responsabilidad del TPSP, cuáles son responsabilidad del cliente, y cualquier responsabilidad entre el cliente y el TPSP. Consulte Sugerencias y herramientas para comprender PCI DSS v4.0 para obtener una plantilla de matriz de responsabilidad que se puede usar para documentar y aclarar cómo se comparten las responsabilidades entre los TPSP y los clientes.

Opciones para que los TPSP Validen el Cumplimiento PCI DSS para los Servicios de los TPSP que Cumplen con los Requisitos de PCI DSS de los Clientes

Los TPSP son responsables de demostrar su cumplimiento con PCI DSS según lo soliciten las organizaciones que gestionan los programas de cumplimiento (por ejemplo, las marcas de pago y los adquirentes). Los TPSP deben ponerse en contacto con las organizaciones de interés para conocer los requisitos.

Cuando un TPSP presta servicios destinados a cumplir o facilitar el cumplimiento de los requisitos de PCI DSS de un cliente o que pueden afectar a la seguridad del CDE de un cliente, estos requisitos entran en el ámbito de las evaluaciones PCI DSS del cliente. Hay dos opciones para que los TPSP validen el cumplimiento en este escenario:

- **Evaluación anual**: El TPSP se somete a una(s) evaluación(es) anual(es) PCI DSS y proporciona pruebas a sus clientes para demostrar que el TPSP cumple con los requisitos aplicables PCI DSS; o
- **Evaluaciones Múltiples a solicitud**: Si un TPSP no se somete a una evaluación anual PCI DSS, debe someterse a evaluaciones a solicitud de sus clientes y/o participar en cada una de las evaluaciones PCI DSS de sus clientes, con los resultados de cada revisión facilitados al cliente o a clientes respectivos.

Si el proveedor se somete a su propia evaluación PCI DSS, se espera que proporcione pruebas suficientes a sus clientes para verificar que el alcance de la evaluación PCI DSS del proveedor cubrió los servicios aplicables al cliente, y que los requisitos relevantes PCI DSS fueron examinados y determinados en cumplimiento. Si el proveedor dispone de un certificado de cumplimiento PCI DSS (AOC), se espera que el TPSP proporcione el AOC a los clientes que lo soliciten. El cliente también puede solicitar las secciones pertinentes del Reporte de Cumplimiento PCI DSS (ROC) del TPSP. El ROC puede ser redactado para proteger cualquier información confidencial.

Si el TPSP no se somete a su propia evaluación PCI DSS y, por lo tanto, no tiene un ROC, se espera que el TPSP proporcione pruebas específicas relacionadas con los requisitos aplicables PCI DSS, de modo que el cliente (o su Asesor) pueda confirmar que el TPSP cumple con esos requisitos de PCI DSS.

Presencia de los TPSP en la(s) Lista(s) de Marca de Pago de Proveedores de Servicio en Cumplimiento

Para un cliente que esté monitoreando el estatus de cumplimiento de un TPSP de conformidad con el Requisito 12.8, la presencia del TPSP en la lista de marca de pago de proveedores de servicios en cumplimiento con PCI DSS ***puede ser prueba suficiente*** del estado de cumplimiento del TPSP si está claro en la lista que los servicios aplicables al cliente fueron cubiertos por la evaluación PCI DSS del TPSP. Si no está claro en la lista, el cliente debe obtener otra confirmación por escrito que aborde el estado de cumplimiento PCI DSS del TPSP.

Para un cliente que busque pruebas del cumplimiento PCI DSS para los requisitos que un TPSP cumple en nombre del cliente o cuando el servicio prestado pueda afectar a la seguridad del CDE del cliente, la presencia del TPSP en la lista de proveedores de servicios conformes con PCI DSS de una marca de pago ***no constituye suficiente evidencia*** de que los requisitos aplicables PCI DSS para ese TPSP se hayan incluido en la evaluación. Si el TPSP dispone de un PCI DSS AOC, se espera que lo facilite a los clientes que lo soliciten.

5 Mejores Prácticas para la Implementación PCI DSS en Procesos Habituales

Una entidad que implementa procesos de negocio tradicionales también conocidos como BAU, como parte de su estrategia global de seguridad, está tomando medidas para garantizar que los controles de seguridad que se han implementado para asegurar los datos y un entorno siguen siendo implementados correctamente y funcionando adecuadamente como curso normal de los negocios.

Algunos de los requisitos de PCI DSS pretenden servir como procesos BAU mediante la supervisión de los controles de seguridad para garantizar su eficacia de forma continua. Esta supervisión por parte de la entidad ayuda a proporcionar una garantía razonable de que la conformidad de su entorno se mantiene entre las evaluaciones PCI DSS. Aunque actualmente hay algunos requisitos BAU definidos en el estándar, donde una entidad debe adoptar procesos BAU adicionales específicos para su organización y entorno cuando sea posible. Los procesos BAU son una forma de verificar que los controles automatizados y manuales funcionan como se espera. Independientemente de si un requisito de PCI DSS es automatizado o manual, es importante que los procesos BAU detecten anomalías, y alerten e informen para que las personas responsables aborden la situación de manera oportuna.

Entre los ejemplos de cómo debe incorporarse lo PCI DSS a las actividades BAU se incluyen, entre otros, los siguientes:

- Asignar la responsabilidad general y la rendición de cuentas del cumplimiento PCI DSS a una persona o equipo. Esto puede incluir estatutos definidos por la dirección ejecutiva para un programa específico de cumplimiento PCI DSS y la comunicación a la dirección ejecutiva.
- Desarrollar métricas de rendimiento para medir la eficacia de las iniciativas de seguridad y la supervisión continua de los controles de seguridad, incluidos aquellos de los que mucho se depende, como los controles de seguridad de la red, los sistemas de detección de intrusos/sistemas de prevención de intrusos (IDS/IPS), los mecanismos de detección de cambios, las soluciones de protección contra programas maliciosos y los controles de acceso, para garantizar que funcionan de forma eficaz y según lo previsto.
- Revisar los datos registrados con mayor frecuencia para obtener información sobre tendencias o comportamientos que pueden no ser obvios sólo con la supervisión.
- Garantizar que todas las fallas en los controles de seguridad se detectan y se responden con prontitud. Los procesos para responder a las fallas de los controles de seguridad deben incluir:
  - Restablecer el control de seguridad.
  - Identificar la causa de la falla.
  - Identificar y abordar cualquier problema de seguridad que haya surgido durante la falla en el control de seguridad.
  - Aplicar medidas de mitigación, como controles técnicos o de procesos, para impedir que se repita la causa de la falla.
  - Reanudar el monitoreo del control de seguridad, tal vez con monitoreo reforzado durante un período de tiempo, para verificar que el control funciona eficazmente.

- Revisar los cambios que podrían introducir riesgos de seguridad en el entorno (por ejemplo, la adición de nuevos sistemas, los cambios en la configuración del sistema o de la red) antes de completar el cambio, e incluir lo siguiente:
  - Realizar una evaluación de riesgos para determinar el impacto potencial en el ámbito PCI DSS (por ejemplo, un nuevo estándar de control de seguridad de la red que permita la conectividad entre un sistema del CDE y otro sistema, podría hacer que otros sistemas o redes entraran en el ámbito PCI DSS).
  - Identificar los requisitos de PCI DSS aplicables a los sistemas y redes afectados por los cambios (por ejemplo, si un nuevo sistema entra en el ámbito PCI DSS, tendría que configurarse según los estándares de configuración del sistema, incluidos los mecanismos de detección de cambios, el software de protección contra programas maliciosos, los parches y el registro de auditoría. Estos nuevos sistemas y redes tendrían que añadirse al inventario de componentes de sistemas incluidos en el ámbito de aplicación y al programa de exploración trimestral de vulnerabilidades).
  - Actualizar el alcance PCI DSS y aplicar los controles de seguridad como sea apropiado.
  - Actualizar la documentación para reflejar los cambios implementados.
- Revisar el impacto en el alcance y los requisitos de PCI DSS en caso de cambios en la estructura organizacional (por ejemplo, una fusión o adquisición de la empresa).
- Revisar periódicamente las conexiones externas y el acceso de terceros.
- En el caso de las entidades que utilizan a terceros para el desarrollo de software, confirmar periódicamente que esas actividades de desarrollo de software siguen cumpliendo los requisitos de desarrollo de software del Requisito 6.
- Realizar revisiones periódicas para confirmar que los requisitos de PCI DSS siguen vigentes y que el personal sigue los procesos establecidos. Las revisiones periódicas deben abarcar todas las instalaciones y ubicaciones, incluidos los puntos de venta y los centros de datos, tanto si son auto-gestionados como si se utiliza un TPSP. Por ejemplo, las revisiones periódicas pueden utilizarse para confirmar que se han aplicado los estándares de configuración a los sistemas aplicables, que se han eliminado o desactivado las cuentas de proveedor predeterminadas y las contraseñas, que los parches y las soluciones contra programas maliciosos están actualizados, que se están revisando los registros de auditoría, etc. Si los requisitos de PCI DSS no indican lo contrario la entidad debe determinar la frecuencia de las revisiones periódicas según el tamaño y complejidad de su entorno.

Estas revisiones también se pueden utilizar para verificar que se mantiene la evidencia necesaria para una evaluación PCI DSS. Por ejemplo, la evidencia de los registros de auditoría, los informes de análisis de vulnerabilidades y las revisiones de las reglas de control de seguridad de la red son necesarios para ayudar a la entidad a prepararse para su próxima evaluación PCI DSS.

- Establecer comunicación con todas las partes afectadas, tanto externas como internas, acerca de las amenazas recientemente identificadas y los cambios en la estructura de la organización. Los materiales de comunicación deben ayudar a los destinatarios a comprender el impacto de las amenazas, los pasos de mitigación y los puntos de contacto para obtener más información o escalar la situación.

- Revisar las tecnologías de hardware y software al menos una vez cada 12 meses para confirmar que continúan siendo respaldadas por el proveedor y pueden cumplir con los requisitos de seguridad de la entidad, incluyendo PCI DSS. Si las tecnologías ya no son compatibles con el proveedor o no pueden satisfacer las necesidades de seguridad de la entidad, la entidad debe preparar un plan de remediación, incluyendo el reemplazo de la tecnología, según sea necesario.

***Nota**: Algunas de las mejores prácticas en esta sección también se incluyen como requisitos de PCI DSS para determinadas entidades. Por ejemplo, aquellos que se someten a una evaluación completa PCI DSS, los proveedores de servicios que validan los requisitos adicionales de "solo proveedor de servicios" y las entidades designadas que deben validar de acuerdo con el Apéndice A3: Validación Complementaria de Entidades Designadas.*

Cada entidad debe considerar implementar estas mejores prácticas en su entorno, incluso si no está obligada a validarlas (por ejemplo, comerciantes que se someten a una autoevaluación).

Consulte *Mejores Prácticas para Mantener el Cumplimiento PCI DSS* en la Biblioteca de Documentos en el sitio web PCI SCC para obtener orientación adicional.

6 Para Asesores: Muestreo para Evaluaciones PCI DSS

El muestreo es una opción para los asesores que realizan evaluaciones PCI DSS para facilitar el proceso de evaluación cuando hay una gran cantidad de elementos en una población que está siendo probada.

Si bien es aceptable que un asesor tome muestras de elementos similares en una población que está siendo probada como parte de su revisión del cumplimiento PCI DSS de una entidad, no es aceptable que una entidad aplique los requisitos de PCI DSS solo a una muestra de su entorno (por ejemplo, los requisitos para los análisis trimestrales de vulnerabilidades se aplican a todos los componentes del sistema). Igualmente, no es aceptable que un asesor revise solo una muestra de los requisitos de PCI DSS para verificar el cumplimiento.

Si bien el muestreo permite a los asesores probar menos del 100% de una población de muestreo determinada, los asesores siempre deben esforzarse por lograr la revisión más completa posible. Se alienta a los asesores a utilizar procesos automatizados u otros mecanismos si la población completa, independientemente de su tamaño, si pueda evaluarse de manera rápida y eficiente con un impacto mínimo en los recursos de la entidad que se evalúa. Cuando no se dispone de procesos automatizados para analizar al 100% de una población, el muestreo es un enfoque igualmente aceptable.

Después de considerar el alcance general, la complejidad y la consistencia del entorno que se está evaluando, y la naturaleza (automatizada o manual) de los procesos utilizados por una entidad para cumplir con un requisito, el asesor puede seleccionar de forma independiente muestras representativas de las poblaciones que se están revisando con el fin de evaluar el cumplimiento de la entidad con los requisitos de PCI DSS. Las muestras deben ser una selección representativa de todas las variantes de la población y deben ser lo suficientemente grandes para proporcionar al asesor la seguridad de que los controles se implementan como se espera en toda la población. Cuando se esté probando el desempeño periódico de un requisito (por ejemplo, semanal o trimestralmente, o periódicamente), el asesor debe intentar seleccionar una muestra que represente el período completo cubierto por la evaluación para que el asesor pueda emitir un juicio razonable de que el requisito se cumplió durante todo el periodo de evaluación. Probar la misma muestra de elementos año tras año podría llevar a que las variaciones desconocidas en los elementos no incluidos en la muestra no sean detectadas. Los asesores deben revalidar la justificación del muestreo para cada evaluación y considerar conjuntos de muestras anteriores. Deben seleccionarse diferentes muestras para cada evaluación.

La selección adecuada de la muestra depende de lo que se considere al examinar a los miembros de la muestra. Por ejemplo, determinar la presencia de antimalware en servidores que se sabe que están afectados por software malintencionado puede llevar a determinar que la población son todos los servidores del entorno o todos los servidores del entorno que ejecutan un determinado sistema operativo, o todos los servidores que no son computadores centrales, etc. La selección de una muestra adecuada incluiría representantes de TODOS los miembros de la población identificada, incluidos todos los servidores que ejecutan el sistema operativo identificado, incluidas todas las versiones, así como los servidores dentro de la población que se utilizan para diferentes funciones (servidor web, servidores de aplicaciones, bases de datos, servidores, etc.).

En caso de que se esté considerando un elemento de configuración específico, la población podría dividirse adecuadamente e identificarse grupos de muestra separados. Por ejemplo, una muestra de todos los servidores puede no ser apropiada cuando se revisa la configuración de un sistema operativo, donde diferentes sistemas operativos están presentes en el entorno. En este caso, las muestras de cada tipo de sistema operativo serían apropiadas para identificar que la configuración se ha establecido de manera apropiada para cada sistema

operativo. Cada conjunto de muestras debe incluir servidores que sean representativos de cada tipo de sistema operativo, incluida la versión, así como funciones representativas.

Otros ejemplos de muestreo incluyen selecciones de personal con roles similares o variados, según el requisito que se evalúa, por ejemplo, una muestra de administradores frente a una muestra de todos los empleados.

Se requiere que el asesor utilice su juicio profesional en la planificación, el desempeño y la evaluación de la muestra para respaldar su conclusión sobre si la entidad ha cumplido con un requisito y cómo lo ha hecho. El objetivo del asesor en el muestreo es obtener suficiente evidencia para obtener una base razonable para dar su opinión. Al seleccionar muestras de forma independiente, los asesores deben considerar lo siguiente:

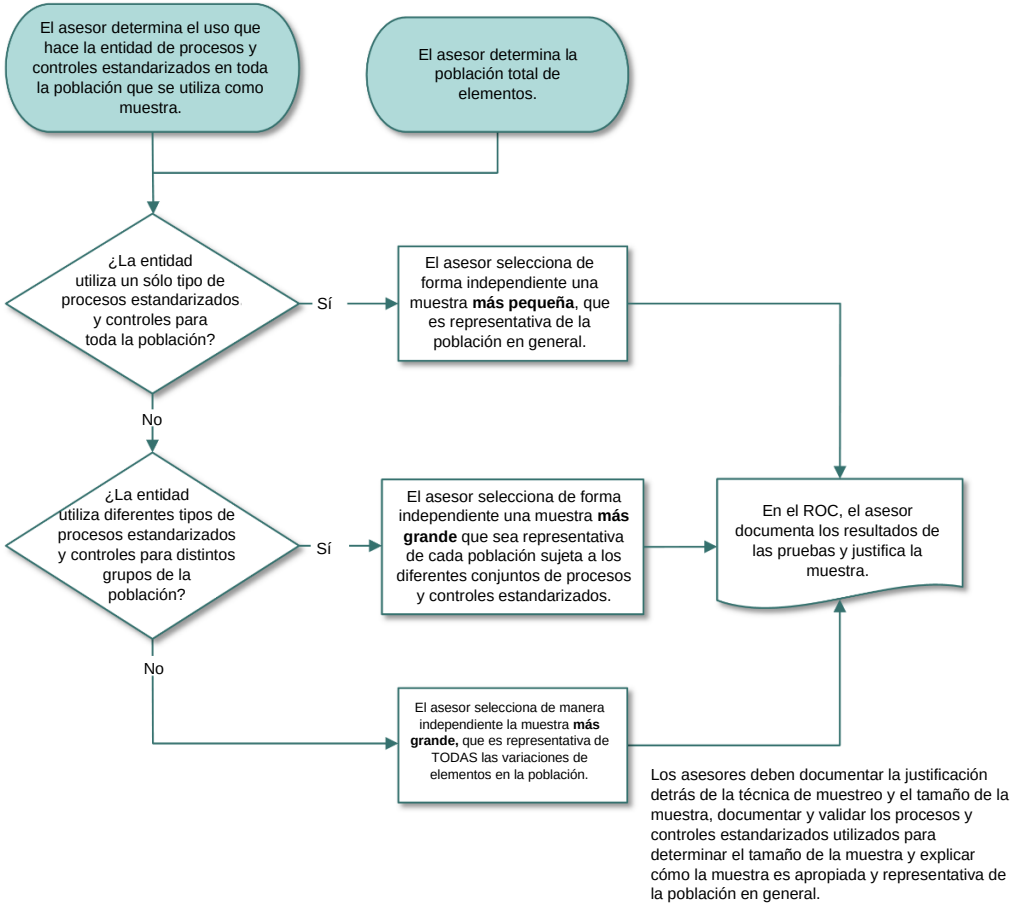
- El asesor debe seleccionar la muestra de la población completa sin influencia de la entidad evaluada.
- Si la entidad cuenta con procesos y controles estandarizados que garanticen la coherencia y que esto se aplica a cada elemento de la población, la muestra puede ser más pequeña que si la entidad no tuviera procesos/controles estandarizados. La muestra debe ser lo suficientemente grande para proporcionar al asesor una seguridad razonable de que los elementos de la población se adhieren a los procesos estandarizados que se aplican a cada elemento de la población. El asesor debe verificar que los controles estandarizados se implementen y funcionen de manera eficiente.
- Si la entidad cuenta con más de un tipo de proceso estandarizado (por ejemplo, para diferentes tipos de instalaciones de negocios/componentes del sistema), la muestra debe incluir elementos sujetos a cada tipo de proceso. Por ejemplo, las poblaciones podrían dividirse en sub-poblaciones según las características que pueden afectar la coherencia de los requisitos evaluados, como el uso de diferentes procesos o herramientas. Luego se seleccionarían muestras de cada subpoblación.
- Si la entidad no cuenta con procesos/controles estandarizados PCI DSS y cada elemento de la población se gestiona mediante procesos no estandarizados, la muestra debe ser mayor para que el asesor tenga la seguridad de que los requisitos de PCI DSS se aplican adecuadamente a cada elemento en la población.
- Las muestras de componentes del sistema deben incluir todos los tipos y combinaciones que se utilicen. Cuando una entidad tiene más de un CDE, las muestras deben incluir poblaciones en todos los componentes del sistema dentro del alcance. Por ejemplo, cuando se trabaje con aplicaciones como muestra, esta debe incluir todas las versiones y plataformas para cada tipo de aplicación.
- Los tamaños de las muestras siempre deben ser mayores a uno, a menos que sólo haya un elemento en la población dada, o que se utilice un control automatizado cuando el asesor haya confirmado que el control está funcionando según lo programado para cada población de muestra evaluada.
- Si el asesor confía en la existencia de procesos y controles estandarizados como base para seleccionar una muestra, pero luego descubre durante las pruebas que los procesos y controles estandarizados no están implementados o no funcionan de manera eficiente, el asesor debe aumentar el tamaño de la muestra para intentar asegurarse de que se cumplen los requisitos de PCI DSS.

Para cada caso en el que se utilice el muestreo, el asesor debe:

- Documentar la justificación de la técnica de muestreo y el tamaño de la muestra.
- Validar y documentar los procesos y controles estandarizados utilizados para determinar el tamaño de la muestra.
- Explicar cómo la muestra es apropiada y representativa de la población en general.

La Figura 3 muestra las consideraciones para determinar el tamaño de la muestra.

Figura 3. Consideraciones de Muestreo PCI DSS



***Nota**: En PCI DSS v4.0 se han eliminado las referencias específicas al muestreo de todos los procedimientos de prueba. Estas referencias se eliminaron porque el hecho de mencionar el muestreo sólo en algunos procedimientos de comprobación podía implicar que el muestreo era obligatorio para esos procedimientos de comprobación (lo cual no era así) o que el muestreo sólo se permitía cuando se mencionaba específicamente. Los asesores deberían seleccionar las muestras cuando sea apropiado, para la población que se está probando y, según lo indicado anteriormente, tomar esas decisiones después de considerar el alcance y la complejidad general de un entorno.*

7 Descripción de los Plazos Utilizados en los Requisitos de PCI DSS

Algunos requisitos de PCI DSS se han establecido con plazos específicos para las actividades que deben realizarse de forma coherente a través de un proceso programado y repetible. La intención es que la actividad se desarrolle en un intervalo lo más cercano posible a ese plazo sin excederlo. La entidad tiene la facultad de realizar una actividad con más frecuencia de la especificada (por ejemplo, realizar una actividad mensualmente, aunque el requisito de PCI DSS especifique que se realice cada tres meses).

La tabla 4 resume la frecuencia de los diferentes periodos de tiempo utilizados en los requisitos de PCI DSS.

Tabla 4. Plazos de los Requisitos de PCI DSS

Plazos en los Requisitos de PCI DSS	Descripciones y ejemplos
Diario	Todos los días del año (no sólo los días laborables).
Semanalmente	Al menos una vez cada siete días.
Mensualmente	Al menos una vez cada 30 o 31 días, o el n° del día del mes.
Cada tres meses ("trimestral")	Al menos una vez cada 90 a 92 días, o el n° del día de cada tercer mes.
Cada seis meses	Al menos una vez cada 180 a 184 días, o el n° del día de cada sexto mes.
Cada 12 meses ("anualmente")	Al menos una vez cada 365 días (o 366 para los años bisiestos) o en la misma fecha cada año.
Periódicamente	La frecuencia de ocurrencia queda a discreción de la entidad y está documentada y respaldada por el análisis de riesgos de la entidad. La entidad debe demostrar que la frecuencia es adecuada para que la actividad sea efectiva y cumpla con la intención del requisito.
Inmediatamente	Sin demora. En tiempo real o casi en tiempo real.
Con prontitud	Tan pronto como sea razonablemente posible.

Plazos en los Requisitos de PCI DSS	Descripciones y ejemplos
Cambio significativo	Hay ciertos requisitos cuyo cumplimiento se especifica cuando se produce un cambio significativo en el entorno de una entidad. Si bien lo que constituye un cambio significativo depende en gran medida de la configuración de un entorno determinado, cada una de las siguientes actividades, como mínimo, tiene impactos potenciales en la seguridad del CDE y debe considerarse como un cambio significativo en el contexto de los requisitos de PCI DSS relacionados: • Nuevo hardware, software o equipo de red añadido al CDE. • Cualquier sustitución o actualización importante de hardware y software en el CDE. • Cualquier cambio en el flujo o almacenamiento de datos de cuentas. • Cualquier cambio en los límites del CDE y/o en el alcance de la evaluación PCI DSS. • Cualquier cambio en la infraestructura de apoyo subyacente del CDE (incluidos, pero sin limitarse a, los cambios en los servicios de directorio, los servidores de tiempo, el registro y la supervisión). • Cualquier cambio en los vendedores/proveedores de servicios (o servicios prestados) que apoyen el CDE o cumplan los requisitos de PCI DSS en nombre de la entidad.

En el caso de otros requisitos de PCI DSS, en los que el estándar no define una frecuencia mínima para las actividades recurrentes, sino que permite que el requisito se cumpla "periódicamente", se espera que la entidad defina la frecuencia según convenga a su negocio. La frecuencia definida por la entidad debe estar respaldada por la política de seguridad de la entidad y el análisis de riesgos realizado de acuerdo con el requisito 12.3.1 PCI DSS. La entidad también debe ser capaz de demostrar que la frecuencia que ha definido es adecuada para que la actividad sea efectiva y cumpla con la intención del requisito.

En ambos casos, cuando PCI DSS especifica una frecuencia requerida y permite un desempeño “periódico", se espera que la entidad tenga procesos documentados e implementados para garantizar que las actividades se realicen dentro de un marco de tiempo razonable, incluidos al menos lo siguiente:

- La entidad es notificada de inmediato cada vez que una actividad no se realiza según su calendario definido.
- La entidad determina los eventos que han provocado el incumplimiento de una actividad programada,
- La entidad realiza la actividad tan pronto como sea posible después de que se pierda, y vuelve a programarla o establece un nuevo calendario.
- La entidad emite documentación que demuestre que ocurrieron los elementos anteriores.

Cuando una entidad cuenta con los procesos mencionados para detectar y abordar el incumplimiento de una actividad programada, se permite un enfoque razonable, lo que significa que, si una actividad debe realizarse al menos una vez cada tres meses, la entidad no incumple automáticamente si la actividad se realiza con retraso cuando se ha seguido el proceso de documentación y se siguió el proceso de implementación (según lo indicado anteriormente). Sin embargo, cuando no exista tal proceso y/o la actividad no se haya desarrollado según el calendario previsto debido a un descuido, a una mala gestión o a la falta de seguimiento, la entidad no habrá cumplido el requisito. En

estos casos, el requisito sólo se cumplirá cuando la entidad 1) documente (o vuelva a confirmar) el proceso mencionado anteriormente para garantizar que la actividad programada se realiza a tiempo, 2) restablezca el calendario y 3) aporte pruebas de que la entidad ha realizado la actividad programada al menos una vez según su calendario.

***Nota**: Para una evaluación inicial PCI DSS (lo que significa que una entidad nunca se ha sometido a una evaluación anterior), cuando un requisito tiene un plazo definido dentro del cual debe producirse la actividad, no es necesario que esta se haya realizado para cada uno de esos plazos durante el año anterior, si el asesor verifica que:*

- *La actividad se ha realizado de acuerdo con el requisito aplicable dentro del lapso más reciente (por ejemplo, el período de tres o seis meses más recientes), y*
- *La entidad cuenta con políticas y procedimientos documentados para seguir realizando la actividad dentro del plazo definido.*

Para los años posteriores a la evaluación inicial, la actividad debe haberse realizado al menos una vez dentro de cada plazo requerido. Por ejemplo, una actividad requerida cada tres meses debe haberse realizado al menos cuatro veces durante el año anterior en un intervalo que no supere los 90-92 días.

8 Enfoques para Implementar y Validar PCI DSS

Para apoyar la flexibilidad en el cumplimiento de los objetivos de seguridad, existen dos enfoques para la implementación y validación PCI DSS. Las entidades deben identificar el enfoque que mejor se adapte a su implementación de seguridad y utilizar ese enfoque para validar los controles.

Enfoque Definido

Sigue el método tradicional de implementación y validación PCI DSS y utiliza los Requisitos y Procedimientos de Prueba definidos en el estándar. En el enfoque definido, la entidad implementa los controles de seguridad para cumplir con los requisitos establecidos, y el asesor sigue los procedimientos de prueba definidos para verificar que se han cumplido los requisitos.

El enfoque definido apoya a las entidades que cuentan con controles establecidos que cumplen con los requisitos de PCI DSS. Este enfoque también puede ser adecuado para las entidades que desean una mayor orientación sobre cómo cumplir con los objetivos de seguridad, así como entidades nuevas en seguridad de la información o PCI DSS.

Controles Compensatorios

Como parte del enfoque definido, las entidades que no pueden cumplir con un requisito de PCI DSS explícitamente como se indica debido a una restricción técnica o empresarial legítima y documentada, pueden implementar otros, o *controles compensatorios*, que mitiguen suficientemente el riesgo asociado con el requisito. Anualmente, cualquier control compensatorio debe ser documentado por la entidad, y revisado y validado por el asesor, e incluirlo en el Reporte de Cumplimiento.

Nota: *Para más detalles, refiérase a Anexo B: Controles Compensatorio y Anexo C: Hoja de Trabajo de Controles Compensatorios.*

Enfoque Personalizado

Se centra en el Objetivo de cada requisito de PCI DSS (si procede), permitiendo a las entidades implementar controles para cumplir con el Objetivo del Enfoque Personalizado establecido en el requisito de una manera que no siga estrictamente el requisito definido. Debido a que cada implementación personalizada será diferente, no hay procedimientos de prueba definidos; el asesor debe derivar procedimientos de prueba que sean apropiados para la implementación específica para validar que los controles implementados cumplan con el Objetivo establecido.

Nota: *Para más detalles, refiérase al Anexo D: Enfoque Personalizado y Anexo E: Plantillas de Muestra para Respaldar el Enfoque Personalizado.*

El enfoque personalizado apoya la innovación en las prácticas de seguridad, permitiendo a las entidades una mayor flexibilidad para mostrar cómo sus controles de seguridad actuales cumplen los objetivos PCI DSS. Este enfoque está destinado a las entidades de riesgo maduro que demuestran un sólido enfoque de gestión de riesgos para la seguridad, incluyendo, pero no limitado a, un departamento especializado de gestión de riesgos o un enfoque de gestión de riesgos en toda la organización.

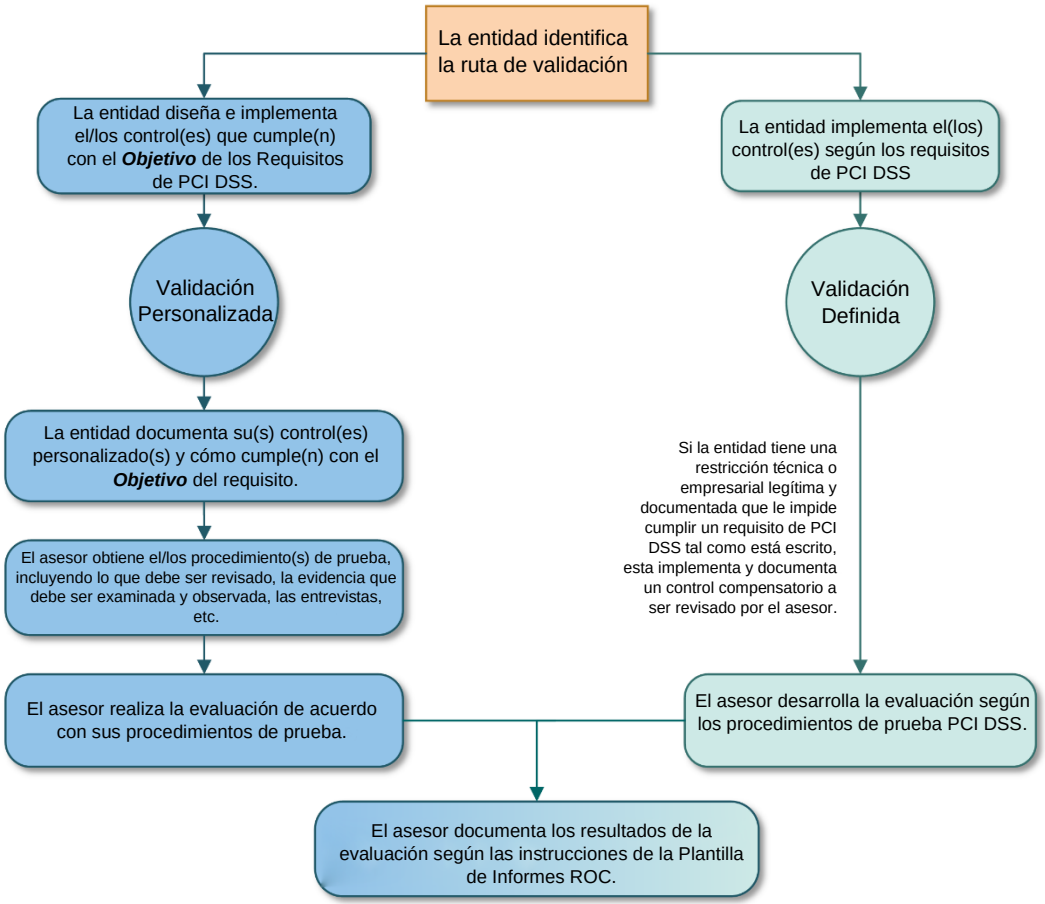
Se espera que los controles implementados y validados utilizando el enfoque personalizado cumplan o superen la seguridad proporcionada por el requisito en el enfoque definido. El nivel de documentación y esfuerzo requerido para validar las implementaciones personalizadas también será mayor que para el enfoque definido.

La mayoría de los requisitos de PCI DSS pueden cumplirse utilizando el enfoque definido o el personalizado. Sin embargo, algunos requisitos no tienen un Objetivo del Enfoque Personalizado establecido; el enfoque personalizado no es una opción para estos requisitos.

Las entidades pueden utilizar tanto el enfoque definido como el personalizado dentro de su entorno. Esto significa que una entidad podría utilizar el enfoque definido para cumplir con algunos requisitos y utilizar el enfoque personalizado para cumplir con otros requisitos. Esto también significa que una entidad podría utilizar el enfoque definido para cumplir un determinado requisito de PCI DSS para un componente del sistema o dentro de un entorno, y utilizar el enfoque personalizado para cumplir ese mismo requisito de PCI DSS para un componente del sistema diferente o dentro de un entorno diferente. De esta manera, una evaluación PCI DSS podría incluir procedimientos de prueba tanto definidos como personalizados.

La Figura 4 muestra las dos opciones de validación para PCI DSS v4.0.

Figura 4. Enfoques de Validación PCI DSS



9 Protección de la Información Acerca de la Postura de la Entidad en Materia de Seguridad

Los procesos relacionados con la obtención y el mantenimiento de un entorno que cumpla con PCI DSS dan lugar a muchos elementos que una entidad puede considerar confidenciales y puede querer proteger como tales, incluyendo elementos como los siguientes:

- El Reporte de Cumplimiento o Cuestionario de Autoevaluación (el Certificado de Cumplimiento asociado no se considera confidencial y se espera que los proveedores de servicios externos (TPSP) compartan su AOC con los clientes).
- Diagramas de red y diagramas de flujo de datos de cuentas, configuraciones y reglas de seguridad.
- Estándares de configuración del sistema.
- Métodos y protocolos de criptografía y gestión de claves.

Las entidades deberían revisar todos los elementos relacionados con los controles PCI DSS o de la evaluación y protegerlos de acuerdo con las políticas de seguridad de la entidad para este tipo de información.

Los TPSP están obligados (requisito 12.9 PCI DSS) a apoyar a sus clientes con lo siguiente:

- Información necesaria para que los clientes puedan supervisar el estado de cumplimiento PCI DSS de los TPSP (para que el cliente pueda cumplir con el requisito 12.8), y
- Evidencia de que el TPSP cumple los requisitos aplicables PCI DSS cuando los servicios del TPSP estén destinados a cumplir o facilitar el cumplimiento de los requisitos de PCI DSS de un cliente, o cuando dichos servicios puedan afectar a la seguridad del CDE de un cliente.

Esta sección no afecta ni niega la obligación de un TPSP de apoyar y proporcionar información a sus clientes según el requisito 12.9.

Para más detalles sobre las expectativas de los TPSP y las relaciones entre los TPSP y los clientes, refiérase al Uso de Proveedores de Servicios Externos.

Protección de la Información Sensible y Confidencial por parte de las Empresas Asesores de Seguridad Certificadas

Cada empresa de asesores de seguridad calificados (QSA) firma un acuerdo con PCI SSC en el que se adherirá a los requisitos de calificación para los QSA. La *sección de Protección de la Información Confidencial y Sensible* de dicho documento incluye lo siguiente:

> "La empresa QSA debe tener y adherirse a un proceso documentado para la protección de la información sensible y confidencial. Este proceso debe incluir las salvaguardas físicas, electrónicas y de procedimiento adecuadas, de acuerdo con las prácticas aceptadas en la industria para proteger la información confidencial y sensible contra cualquier amenaza o acceso no autorizado durante el almacenamiento, el procesamiento y/o la comunicación de esta información.

La empresa QSA deberá mantener la privacidad y la confidencialidad de la información obtenida en el curso del cumplimiento de sus deberes y obligaciones como empresa QSA, a menos que (y en la medida en que lo sea) su divulgación sea requerida por la autoridad legal."

10 Métodos de Prueba para los Requisitos de PCI DSS

Los métodos de prueba identificados en los Procedimientos de Prueba para cada requisito describen las actividades que se espera que realice el asesor para determinar si la entidad ha cumplido con el requisito. La intención de cada método de prueba se describe como sigue:

- Evalué: El asesor examina de forma crítica las evidencias de datos. Algunos ejemplos comunes son los documentos (electrónicos o físicos), las capturas de pantalla, los archivos de configuración, los registros de auditoría y los archivos de datos.
- Observe: El asesor observa una acción o percibe algo en el entorno. Algunos ejemplos de sujetos de observación son el personal que realiza una tarea o un proceso, los componentes del sistema que realizan una función o responden a una entrada, las condiciones ambientales y los controles físicos.
- Entreviste: El asesor entrevista al personal. Los objetivos de la entrevista pueden incluir la confirmación de si se realiza una actividad, las descripciones de cómo se realiza una actividad y si el personal tiene conocimientos particular o comprensión.

Los métodos de prueba tienen el objetivo de permitir a la entidad evaluada demostrar cómo ha cumplido un requisito. También proporcionan a la entidad evaluada y al asesor un entendimiento común de las actividades de evaluación que deben realizarse. Los elementos específicos que deben examinarse u observarse y el personal que debe entrevistarse deben ser adecuados tanto para el requisito que se evalúa como para la implementación particular de cada entidad. Al documentar los resultados de la evaluación, el asesor identifica las actividades de pruebas realizadas y el resultado de cada actividad.

11 Instrucciones y Contenido del Informe de Cumplimiento

Las instrucciones y el contenido del Informe de Cumplimiento (ROC) se proporcionan en la Plantilla para crear el informe del ROC PCI DSS.

La Plantilla para crear informes (ROC) PCI DSS debe utilizarse como plantilla para crear un Informe de Cumplimiento PCI DSS.

Queda a discreción de las organizaciones que administran los programas de cumplimiento (como las marcas de pago y los adquirentes) determinar si alguna entidad está sujeta a cumplir o validar su cumplimiento con PCI DSS Las entidades deben ponerse en contacto con las organizaciones de interés para determinar los requisitos e instrucciones del informe.

12 Proceso de Evaluación PCI DSS

El proceso de evaluación PCI DSS incluye los siguientes pasos de alto nivel:[5]

1. Confirme el alcance de la evaluación PCI DSS.
2. Realice la evaluación del entorno PCI DSS.
3. Complete el informe correspondiente para la evaluación de acuerdo con las guías e instrucciones PCI DSS.
4. Complete la Declaración de Cumplimiento para Proveedores de Servicios o Comerciantes, según corresponda, en su totalidad. Las Declaraciones Oficiales de Cumplimiento solo están disponibles en el sitio web PCI SCC.
5. Envíe la documentación correspondiente PCI SCC y la Certificación de cumplimiento, junto con cualquier otra documentación solicitada, como informes de escaneo ASV, a la organización solicitante (aquellas que administran programas de cumplimiento, como marcas de pago y adquirentes (para comercios) u otros solicitantes (para proveedores de servicios)).
6. Si es necesario, realiza remediaciones para abordar los requisitos que no están en cumplimiento y presente un informe actualizado.

Nota: *No se considera que los requisitos de PCI DSS estén vigentes si los controles no se han implementado aún o si están programados para completarse en el futuro. Una vez que la entidad haya corregido los requerimientos abiertos o que no están en cumplimiento, el asesor volverá a evaluar para validar que se completó la remediación y que se cumplieron todos los requisitos. Consulte los siguientes recursos (disponibles en el sitio web PCI SCC) para documentar la evaluación PCI DSS:*

- *Para obtener instrucciones sobre cómo completar Informes de Cumplimiento (ROC), consulte la Plantilla para crear los Informes de ROC PCI DSS.*
- *Para obtener instrucciones sobre cómo completar cuestionarios de autoevaluación (SAQ), consulte las Instrucciones y guías del SAQ PCI DSS.*
- *Para obtener instrucciones sobre cómo enviar informes de validación de cumplimiento PCI DSS, consulte la Declaración de Cumplimiento PCI DSS.*

[5] El proceso de evaluación PCI DSS y los roles y responsabilidades para completar cada paso varían según el tipo de evaluación y los programas de cumplimiento que son administrados por las marcas de pago y los adquirentes.

13 Referencias Adicionales

La Tabla 5 enumera las organizaciones externas a las que se hace referencia en los requisitos de PCI DSS o en la guía relacionada. Estas organizaciones externas y sus referencias se proporcionan sólo como información y no reemplazan ni amplían ningún requisito de PCI DSS.

Tabla 5. Organizaciones Externas a las que se hace referencia en los requisitos de PCI DSS

Referencia	Nombre Completo	Fuente
ANSI	American National Standards	www.ansi.org
CIS	Center for Internet Security	www.cisecurity.org
CSA	Cloud Security Alliance	www.csa.org
ENISA	European Union Agency for Cybersecurity (Formerly European Network and Information Security Agency)	www.enisa.europa.eu
FIDO Alliance	The FIDO Alliance	www.fidoalliance.org
ISO	International Organization for Standardization	www.iso.org
NCSC	The UK National Cyber Security Centre	www.ncsc.gov.uk
NIST	National Institute of Standards and Technology	www.nist.gov
OWASP	Open Web Application Security Project	www.owasp.org
SAFEcode	Software Assurance Forum for Excellence in Code	www.safecode.org

14 Versiones PCI DSS

A la fecha de publicación de este documento, PCI DSS v3.2.1 son válidos hasta el 31 de marzo de 2024, después de esta fecha se retira. Todas las validaciones PCI DSS después de esta fecha deben ser para PCI DSS 4.0 o posterior.

Se puede utilizar PCI DSS versión 3.2.1 o 4.0 para evaluaciones entre marzo de 2022 y el 31 de marzo de 2024.

La Tabla 6 resume las versiones PCI DSS y sus fechas relevantes.[6]

Tabla 6. Versiones PCI DSS

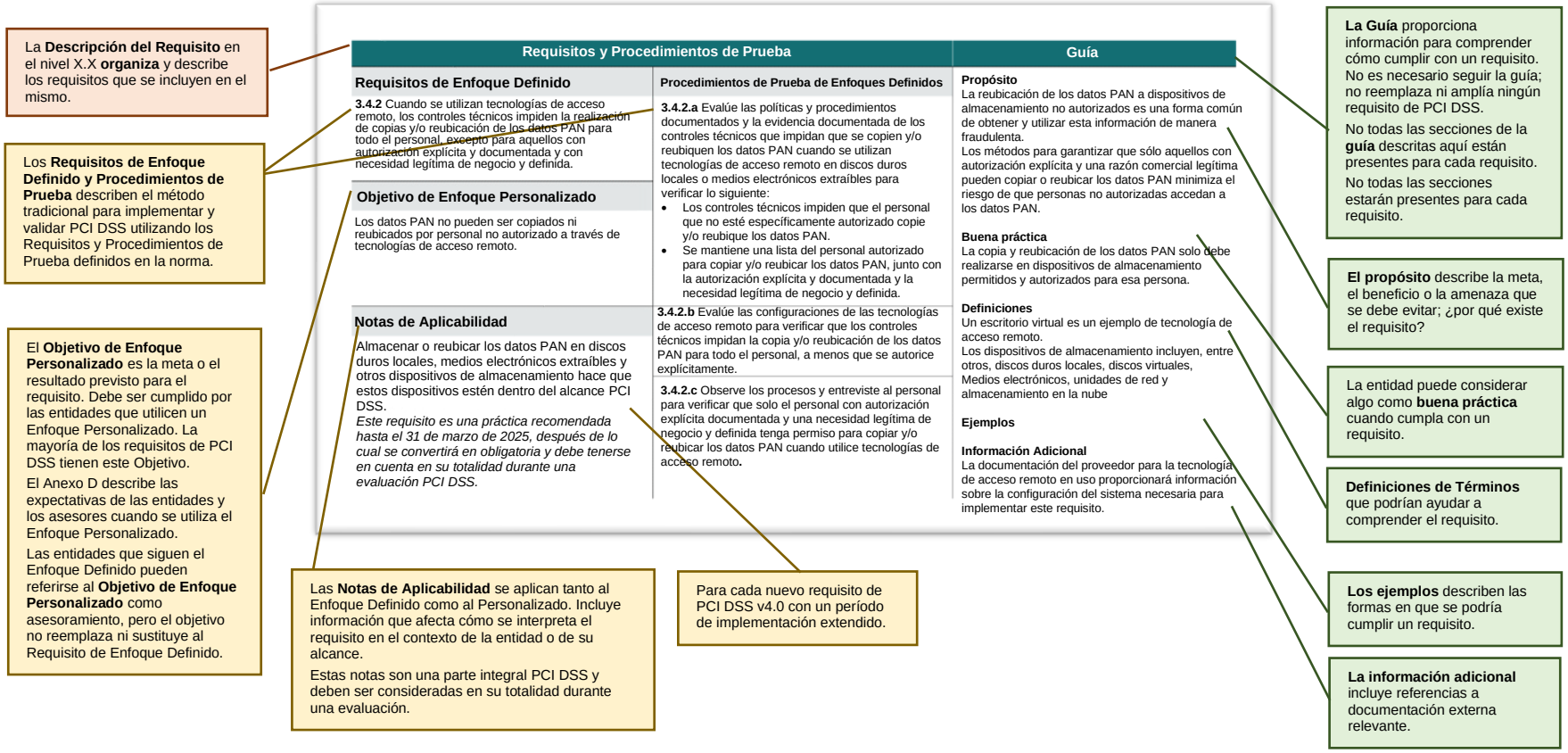
Versión	Publicada	Retirada
PCI DSS v4.0 (este documento)	Marzo de 2022	Por determinar
PCI DSS v3.2.1	Mayo de 2018	31 de marzo de 2024

[6] Sujeto a cambios tras el lanzamiento de una nueva versión PCI DSS

15 Procedimientos Detallados de Evaluación de Seguridad y Requisitos de PCI DSS

La Figura 5 describe los encabezados de las columnas y el contenido de los requisitos de PCI DSS.

Figura 5. Comprensión de las Partes del Estándar



Requisitos Adicionales sólo para Proveedores de Servicios

Algunos requisitos se aplican solamente cuando la entidad que se evalúa es un proveedor de servicios. Estos se identifican dentro del requisito como "*Requisito adicional solo para proveedores de servicios"* y se aplican adicionalmente a todos los demás requisitos aplicables. Cuando la entidad que se evalúa es tanto un comercio como también un proveedor de servicios, los requisitos señalados como "*Requisitos adicionales sólo para proveedores de servicios"* se aplican a la porción o sección de proveedor de servicios del negocio de la entidad. Los requisitos identificados con "*Requisito adicional sólo para proveedores de servicios"* también se recomiendan como mejores prácticas a ser consideradas por todas las entidades.

Anexos con los Requisitos Adicionales PCI DSS para Diferentes Tipos de Entidades

Además de los 12 requisitos principales, el Anexo A PCI DSS contiene requisitos adicionales PCI DSS para diferentes tipos de entidades. Las secciones dentro del Anexo A incluye:

- Anexo A1: Requisitos Adicionales de PCI DSS para Proveedores de Servicios Multiusuario.
- Anexo A2: Requisitos Adicionales de PCI DSS Para Entidades que Utilizan SSL/Primeras Versiones de TLS para Conexiones de Terminal POS POI Presencial con Tarjetas.
- Anexo A3: Validación Complementaria de Entidades Designadas (DESV).

Construir y Mantener Redes y Sistemas Protegidos

Requisito 1: Instalar y Mantener los Controles de Seguridad de la Red

Secciones	
1.1	Se definen y comprenden los procesos y mecanismos para instalar y mantener los controles de seguridad en la red.
1.2	Se configuran y mantienen los controles de seguridad de la red (NSC, por sus siglas en Ingles).
1.3	El acceso a la red desde y hacia el ambiente de datos del titular de la tarjeta está restringido.
1.4	Se controlan las conexiones de red entre las redes confiables y las redes no confiables.
1.5	Se mitigan los riesgos para el CDE que pueden provenir de los dispositivos informáticos que pueden llegar a conectarse al CDE o a redes no confiables.

Descripción
Los Controles de Seguridad de Red (NSC), como los *firewalls* y otras tecnologías de protección de red, constituyen puntos de implementación de políticas de red que suelen controlar el tráfico de red entre dos o más segmentos lógicos o físicos (o sub-redes) basándose en *políticas o reglas* predefinidas. Los NSC examinan todo el tráfico de red que entra (acceso) y sale (egresa) de un segmento y deciden, basándose en las políticas o reglas definidas, ya sea que el tráfico de red está permitido o si debe ser rechazado. Comúnmente, los NSC se implementan entre los entornos con distintas necesidades de seguridad o niveles de confiabilidad, sin embargo en algunos ambientes los NSC controlan el tráfico hacia dispositivos individuales independientemente de los límites de confianza. La implementación de las políticas o reglas en los NSC se producen generalmente en la capa 3 del modelo OSI, pero los datos presentes en las capas superiores también se utilizan con frecuencia en las políticas para tomar decisiones de control de tráfico. Tradicionalmente, esta función ha sido proporcionada por *firewalls* físicos; sin embargo, ahora esta funcionalidad puede ser proporcionada por dispositivos virtuales, controles de acceso en la nube, sistemas de virtualización/contenedores y otra tecnología de redes definida por software. Los NSC se utilizan para controlar el tráfico dentro de las propias redes de una entidad, por ejemplo, entre áreas altamente confidenciales y menos confidenciales, y también para proteger los recursos de la entidad de la exposición a redes que no son fiables. El entorno de datos del titular de la tarjeta (CDE) es un ejemplo del área más sensible dentro de la red de una entidad. A menudo, rutas aparentemente insignificantes hacia y desde redes que no son confiables pueden proporcionar rutas desprotegidas hacia sistemas confidenciales. Los NSC proporcionan un mecanismo de protección clave para cualquier red informática. Ejemplos comunes de redes que no son confiables incluyen Internet, conexiones especializadas como canales de comunicación de empresa a empresa, redes inalámbricas, redes de operadores (como celulares), redes de terceros y otras fuentes fuera de la capacidad de control de la entidad. Además, las redes que no son confiables también incluyen redes corporativas que se consideran fuera del alcance PCI DSS, porque no se evalúan y, por lo tanto, deben tratarse como no confiables porque no se ha verificado la existencia de controles de seguridad. Si bien una entidad puede considerar que una red interna es confiable desde la perspectiva de infraestructura, si una red está fuera del alcance PCI DSS, esa red debe considerarse no confiable para PCI DSS. Consulte el Anexo G para acceder a las definiciones de los términos o glosario PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
1.1 Se definen y comprenden los procesos y mecanismos para instalar y mantener los controles de seguridad de la red.		
Requisitos del Enfoque Definido **1.1.1** Todas las políticas de seguridad y los procedimientos operativos que se identifican en el Requisito 1 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y el seguimiento al cumplimiento de las actividades del Requisito 1 son definidos, comprendidos y cumplidos por el personal involucrado. Todas las actividades de soporte son repetibles, se aplican de manera consistente y se ajustan a la intención de la gestión	**Procedimientos de Prueba del Enfoque Definido** **1.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 1 se gestionen de acuerdo con todos los elementos especificados en este requisito.	**Propósito** El requisito 1.1.1 describe la gestión y el mantenimiento eficaz de las distintas políticas y procedimientos especificados en el requisito 1. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 1, es igualmente importante garantizar que se documenten, mantengan y difundan adecuadamente. **Buenas prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocio. Por estas razones, considere la posibilidad de actualizar estos documentos tan pronto como se produzca un cambio y no sólo periódicamente. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que las actividades críticas no ocurran. **Buenas prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme la aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién es el nivel de autoridad, quién es el responsable, persona quien se debe consultar y la persona informa (también llamada matriz RACI).
1.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 1 están documentadas, asignadas y comprendidas.	**1.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y las responsabilidades para realizar las actividades del Requisito 1 están documentadas y asignadas.	
	1.1.2.b Entreviste al personal responsable de realizar las actividades del Requisito 1 para verificar que los roles y responsabilidades son asignados como documentadas y entendidas.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 1. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
1.2 Se configuran y mantienen los controles de seguridad de la red (NSC).		
Requisitos del Enfoque Definido **1.2.1** Los estándares de configuración para el conjunto de reglas de los NSC son: • Definidos. • Implementados. • Mantenidos. **Objetivo del Enfoque Personalizado** La forma en que se configuran y operan los NSC se define y se aplica de manera consistente.	**Procedimientos de Prueba del Enfoque Definido** **1.2.1.a** Evalúe los estándares de configuración para los conjuntos de reglas NSC a fin de verificar que los estándares están de acuerdo con todos los elementos especificados en este requisito. **1.2.1.b** Evalúe los parámetros de configuración del conjunto de reglas de los NSC para verificar que el conjunto de reglas se implementen de acuerdo con los estándares de configuración.	**Propósito** La implementación de estos estándares de configuración tiene como resultado que los NSC estén configurados y gestionados para realizar correctamente su función de seguridad (a menudo denominada conjunto de reglas o rule set). **Buenas prácticas** Estas os estándares suelen definir los requisitos de los protocolos aceptables, los puertos que se pueden utilizar y los requisitos de configuración específicos que son aceptables. Los estándares de configuración también pueden describir lo que la entidad considera no aceptable o no permitido dentro de su red. **Definiciones** Los NSC son componentes clave de una arquitectura de red. Lo más habitual es que los NSC se utilicen dentro de los límites del CDE para controlar el tráfico de red que entra y sale del CDE. Los estándares de configuración describen los requisitos mínimos de una entidad para la configuración de los NSC de la entidad. **Ejemplos** Los ejemplos de NSC cubiertos por estos estándares de configuración incluyen, pero no se limitan a, *firewalls, routers* configurados con listas de control de acceso y redes virtuales en la nube.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Buenas prácticas**
1.2.2 Todos los cambios en las conexiones de red y en las configuraciones de los NSC se aprueban y gestionan de acuerdo con el proceso de control de cambios definido en el Requisito 6.5.1.	**1.2.2.a** Evalúe los procedimientos documentados para verificar que los cambios en las conexiones de red y las configuraciones de los NSC estén incluidos en el proceso formal de control de cambios de acuerdo con el Requisito 6.5.1.	Los cambios deberían ser aprobados por personas con la autoridad y el conocimiento adecuados para comprender el impacto del cambio. La verificación debe proporcionar una garantía razonable de que el cambio no tuvo un impacto adverso en la seguridad de la red y de que el cambio funciona como se esperaba. Para evitar tener que abordar los problemas de seguridad generados por un cambio, todos los cambios deben aprobarse antes de implementarse y verificarse una vez implementado el cambio. Una vez aprobado y verificado, la documentación de la red debe ser actualizada para incluir los cambios evitando que se presenten inconsistencias entre la documentación de la red y la configuración en el ambiente de producción.
	1.2.2.b Evalúe los ajustes de configuración de la red para identificar los cambios realizados en las conexiones de red. Entreviste al personal responsable y Evalúe los registros de control de cambios para verificar que los cambios identificados en las conexiones de red fueron aprobados y gestionados de acuerdo con el Requisito 6.5.1.	
Objetivo del Enfoque Personalizado Los cambios en las conexiones de red y en los NSC no pueden dar como resultado una mala configuración, la implementación de servicios inseguros o conexiones de red no autorizadas.	**1.2.2.c** Evalúe los parámetros de configuración de la red para identificar los cambios realizados en las configuraciones de los NSC. Entreviste al personal responsable y Evalúe los registros de control de cambios para verificar que los cambios identificados en las configuraciones de los NSC fueron aprobados y gestionados de acuerdo con el Requisito 6.5.1.	
Notas de Aplicabilidad Los cambios en las conexiones de red incluyen la adición, eliminación o modificación de una conexión. Los cambios en la configuración del NSC incluyen aquellos relacionados con el propio componente, así como los que afectan la forma en que realiza su función de seguridad.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** El mantenimiento de un diagrama o diagramas de red precisos y actualizados impide que se pasen por alto las conexiones y los dispositivos de la red y que, sin darse cuenta, queden inseguros y vulnerables a los ataques. Los diagramas de red propiamente mantenidos ayudan a una organización a verificar el alcance PCI DSS identificando los sistemas que se conectan hacia y desde el CDE. **Buenas prácticas** Deben identificarse todas las conexiones hacia y desde el CDE, incluyendo los sistemas que proveen servicios de seguridad, gestión o mantenimiento al CDE. Las entidades deben considerar la inclusión de los siguientes aspectos en sus diagramas de red: • Todas las ubicaciones, incluyendo los *retails*, *data centers*, las oficinas corporativas, los proveedores de la nube o *Cloud*, etc. • Un etiquetado claro de todos los segmentos de red. • Todos los controles de seguridad que proporcionan segmentación, incluyendo identificadores únicos para cada control (por ejemplo, nombre del control, marca, modelo y versión). • Todos los componentes del sistema incluidos en el alcance, como los NSC, *firewalls* de aplicaciones web o WAF (Web App Firewall), soluciones antimalware maliciosos, soluciones de gestión de cambios, IDS/IPS, servidores o sistemas de centralización de *logs*, terminales de pago, aplicaciones de pago, HSM, etc. *(continúa en la página siguiente)*
1.2.3 Se mantienen los diagramas de red precisos que muestran todas las conexiones entre el CDE y otras redes, incluyendo las redes inalámbricas.	**1.2.3.a** Evalúe los diagramas de red y observe las configuraciones de la red para verificar que existan diagrama(s) de red precisos y acordes con todos los elementos especificados en este requisito.	
	1.2.3.b Evalúe la documentación y entreviste al personal responsable para verificar que los diagramas de red sean precisos y estén actualizados cuando se realicen cambios en el ambiente.	
Objetivo del Enfoque Personalizado		
Se mantiene y permanece disponible una representación (Ej. Diagrama) de los límites entre el CDE, todas las redes confiables y todas las redes no confiables.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Se puede utilizar un(os) diagrama(s) de red vigente(s) u otra solución técnica o topológica que identifique las conexiones y dispositivos en la red para cumplir con este requisito.		• Identificación y etiquetado claro de cualquier área fuera del alcance en el diagrama, mediante un cuadro sombreado u otro mecanismo. • Fecha de la última actualización, y nombres de las personas que realizaron y aprobaron las actualizaciones. • Una narrativa o descripción para explicar el diagrama. Los diagramas deben ser actualizados por personal autorizado para asegurarse de que continúen proporcionando una descripción precisa de la red.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **1.2.4** Se mantienen diagramas de flujo de datos precisos que cumplen con lo siguiente: • Muestran todos los flujos de datos de la cuenta a través de los sistemas y las redes involucradas. • Se actualizan según sea necesario ante cambios en el ambiente. **Objetivo del Enfoque Personalizado** Se mantiene y está disponible una representación (Ej. Diagrama) de todas las transmisiones de datos de cuenta entre los componentes del sistema y entre los segmentos de la red involucrados. **Notas de Aplicabilidad** Para cumplir con este requisito la entidad puede utilizar un diagrama de flujo de datos u otra solución técnica o topológica que identifique los flujos de datos de cuenta a través de los sistemas y las redes.	**Procedimientos de Prueba del Enfoque Definido** **1.2.4.a** Evalúe los diagramas de flujo de datos y entreviste al personal para verificar que los diagramas muestren todos los flujos de datos de la cuenta de acuerdo con todos los elementos especificados en este requisito. **1.2.4.b** Evalúe la documentación y entreviste al personal responsable para verificar que los diagramas de flujo de datos sean precisos y estén actualizados cuando haya cambios en el entorno.	**Propósito** Un diagrama de flujo de datos actualizado y fácilmente disponible ayuda a la organización a comprender y realizar un seguimiento del alcance de su entorno al mostrar cómo fluyen los datos de la cuenta a través de las redes y entre los sistemas y dispositivos individuales. Mantener diagrama(s) de flujo de datos actualizado(s) impide que los datos de la cuenta se ignoren y omitan y, sin darse cuenta, queden sin la seguridad requerida. **Buenas prácticas** El diagrama de flujo de datos debe incluir todos los puntos de conexión donde los datos de la cuenta se reciben y se envían fuera de la red, incluidas las conexiones a redes abiertas, públicas, flujos de procesamiento de aplicaciones, almacenamiento, transmisiones entre sistemas y redes, y copias de seguridad de archivos. El diagrama de flujo de datos está destinado a ser adicional al diagrama de red y debe ser consistente con el diagrama de red y complementarlo. Como buena práctica, las entidades pueden considerar incluir lo siguiente en sus diagramas de flujo de datos: • Todos los flujos de procesamiento de los datos de la cuenta, incluida la captura autorización, liquidación, contra cargos y reembolsos. • Todos los canales de aceptación de pagos, incluyendo los de tarjeta presente, tarjeta no presente y de comercio electrónico. • Todos los tipos de recepción o transmisión de datos de tarjeta, incluidos los que involucran copias impresas o soportes en papel. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
		• El flujo de datos de la cuenta desde el punto donde ingresa al ambiente, hasta su disposición final. • Donde se transmiten y procesan los datos de la cuenta, donde se almacenan y si el almacenamiento es a corto o a largo plazo. • La fuente de todos los datos de la cuenta recibidos (por ejemplo, clientes, terceros, etc.) y cualquier entidad con la que se comparten los datos de la cuenta. • Fecha de la última actualización, y nombres de las personas que realizaron y aprobaron las actualizaciones.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.2.5 Todos los servicios, protocolos y puertos permitidos están identificados, aprobados y tienen una necesidad de negocio definida.	**1.2.5.a** Evalúe la documentación para verificar que existe una lista de todos los servicios, protocolos y puertos permitidos, incluyendo la justificación de negocio y la aprobación para cada uno.	Las fallas de seguridad a menudo ocurren debido a servicios, puertos y protocolos no utilizados o inseguros (por ejemplo, telnet y FTP), ya que estos pueden llevar a que se abran puntos de acceso innecesarios dentro o en el entorno del CDE. Además, los servicios, protocolos y puertos que están habilitados pero que no se utilizan a menudo pueden ser ignorados y quedan sin asegurar y sin parchar. Al identificar los servicios, protocolos y puertos necesarios para el negocio, las entidades pueden asegurarse de que todos los demás servicios, protocolos y puertos están desactivados o eliminados.
Objetivo del Enfoque Personalizado	**1.2.5.b** Evalúe los parámetros de configuración de los NSC para verificar que sólo se utilizan los servicios, protocolos y puertos aprobados.	**Buenas prácticas**
El tráfico de red no autorizado (servicios, protocolos o paquetes destinados a puertos específicos) no puede entrar o salir de la red.		Se debe comprender el riesgo de seguridad asociado a cada servicio, protocolo y puerto permitido. Las aprobaciones deben ser concedidas por personal independiente de los que gestionan la configuración y/o administradores de sistemas. El personal encargado de la aprobación debe poseer los conocimientos y contar con la responsabilidad adecuados para tomar las decisiones de aprobación.

<table>
<tr><th colspan="2">Requisitos y Procedimientos de Prueba</th><th>Guía</th></tr>
<tr><td>Requisitos del Enfoque Definido</td><td>Procedimientos de Prueba del Enfoque Definido</td><td rowspan="4">Propósito
Las fallas de seguridad prosperan en las configuraciones de red inseguras.
Buenas prácticas
Si los servicios, protocolos o puertos inseguros son necesarios para el negocio, el riesgo que suponen estos servicios, protocolos y puertos debe ser claramente entendido y aceptado por la organización, el uso del servicio, protocolo o puerto debe estar justificado, y las configuraciones de seguridad que mitigan el riesgo de usar estos servicios, protocolos y puertos deben ser definidas e implementadas por la entidad.
Información adicional
Para obtener orientación sobre los servicios, protocolos o puertos considerados inseguros, consulte los estándares y guías del sector (por ejemplo, del NIST, ENISA, OWASP).</td></tr>
<tr><td rowspan="2">1.2.6 Las configuraciones de seguridad son definidas e implementadas para todos los servicios, protocolos y puertos que están en uso y que son considerados inseguros, de tal manera que el riesgo es mitigado.</td><td>1.2.6.a Evalúe la documentación que identifica todos los servicios, protocolos y puertos inseguros en uso para verificar que para cada uno de ellos se definen configuraciones de seguridad para mitigar el riesgo.</td></tr>
<tr><td>1.2.6.b Evalúe los parámetros configuración de los NSC para verificar que las configuraciones de seguridad definidas hayan sido implementadas para cada servicio, protocolo y puerto inseguro identificado.</td></tr>
<tr><td>Objetivo del Enfoque Personalizado</td><td></td></tr>
<tr><td>Los riesgos específicos asociados con el uso de servicios, protocolos y puertos inseguros son entendidos, evaluados y mitigados apropiadamente.</td><td></td><td></td></tr>
</table>

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
1.2.7 Las configuraciones de los NSC se revisan al menos una vez cada seis meses para confirmar que son pertinentes y eficientes.	**1.2.7.a** Evalúe la documentación para verificar que se han definido procedimientos para revisar las configuraciones de los NSC al menos una vez cada seis meses.	**Propósito** Esta revisión da a la organización la oportunidad de depurar cualquier regla innecesaria, obsoleta o incorrecta y configuraciones que podrían ser utilizadas por personas no autorizadas. Además, garantiza que todas las reglas y configuraciones permitan solamente los servicios, protocolos y puertos autorizados que coincidan con las justificaciones de negocio documentadas. **Buenas prácticas** Esta revisión, que puede implementarse mediante métodos manuales, automatizados o basados en el sistema, pretende confirmar que las configuraciones que controlan las reglas de tráfico, solo permiten la entrada y salida del tráfico que coinciden con las configuraciones aprobadas. La revisión debería proporcionar la confirmación de que todos los accesos permitidos tienen una razón de negocio justificada. Cualquier inconsistencia o duda sobre una regla o configuración debe ser escalada para su resolución. Aunque este requisito especifica que esta revisión se realice al menos una vez cada seis meses, las organizaciones con un alto volumen de cambios en sus configuraciones de red pueden considerar realizar revisiones con mayor frecuencia para garantizar que las configuraciones siguen satisfaciendo las necesidades del negocio.
	1.2.7.b Evalúe la documentación de las revisiones de las configuraciones de los NSC y entreviste al personal responsable para verificar que las revisiones se realizan al menos una vez cada seis meses.	
Objetivo del Enfoque Personalizado Las configuraciones del NSC que permiten o restringen el acceso a las redes confiables se verifican periódicamente para garantizar que sólo se permiten las conexiones autorizadas con una justificación de negocio actual.	**1.2.7.c** Evalúe las configuraciones para los NSC para verificar que las configuraciones identificadas como no soportadas por una justificación de negocios sean removidas o actualizadas.	

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Para impedir que se apliquen configuraciones no autorizadas a la red, los archivos almacenados con las configuraciones para controles de red deben mantenerse actualizados y protegidos contra cambios no autorizados. El mantener la información de la configuración actualizada y segura garantiza que se apliquen los ajustes correctos para los NSC cada vez que se ejecute la configuración. **Ejemplos** Si las configuraciones seguridad de un *router* se almacenan en una memoria no volátil, cuando ese *router* se reinicie o intente cargar desde el archivo de configuración desde dicha memoria, estos controles deberían garantizar que las configuraciones de seguridad sean restablecidas.
1.2.8 Los archivos de configuración de los NSC están: • Asegurados contra el acceso no autorizado. • Se mantienen consistentes con las configuraciones de red activas.	**1.2.8** Evalúe los archivos de configuración de los NSC para verificar que cumplen con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado Las configuraciones de los NSC donde estén ubicadas deben ser protegidas para evitar accesos no autorizados e inconsistencias frente a las configuraciones de seguridad adoptadas por la entidad (incluyendo archivos de configuración)		
Notas de Aplicabilidad Cualquier archivo o ajuste utilizado para configurar o sincronizar los NSC se considera un "archivo de configuración". Esto incluye archivos, controles automatizados y basados en el sistema, scripts, configuraciones, infraestructura como código u otros parámetros de los que se hace una copia de seguridad, se archivan o se almacenan de forma remota.		

Requisitos y Procedimientos de Prueba		Guía
1.3 El acceso a la red hacia y desde el entorno de datos del titular de la tarjeta está restringido.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.3.1 El tráfico de entrada al CDE está restringido de la siguiente manera: • Sólo al tráfico necesario. • Todo el resto del tráfico está explícitamente denegado.	**1.3.1.a** Evalúe los estándares de configuración de los NSC para verificar que definen las restricciones del tráfico de entrada al CDE de acuerdo con todos los elementos especificados en este requisito.	Este requisito tiene por objetivo prevenir que personas malintencionadas accedan a la red de la entidad a través de direcciones IP no autorizadas o que utilicen servicios, protocolos o puertos de forma no autorizada. **Buenas prácticas** Todo el tráfico entrante al CDE, independientemente de su origen, debe ser evaluado para garantizar que sigue las reglas establecidas y autorizadas. Las conexiones deben ser inspeccionadas para asegurar que el tráfico está restringido sólo a las comunicaciones autorizadas-por ejemplo, restringiendo las direcciones específicas de origen/destino puertos, y bloqueando el tráfico. **Ejemplos** Implementar una regla que rechace todo el tráfico entrante y saliente que no sea específicamente necesario -por ejemplo, utilizando una declaración explícita de "denegar todo" o implícita de denegar después de permitir- ayuda a impedir agujeros involuntarios potencialmente dañinos.
Objetivo del Enfoque Personalizado El tráfico no autorizado no puede entrar en el CDE.	**1.3.1.b** Evalúe las configuraciones de los NSC para verificar que el tráfico de entrada al CDE es restringido de acuerdo con todos los elementos especificados en este requerimiento.	

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.3.2 El tráfico saliente del CDE se restringe de la siguiente manera: • Sólo al tráfico necesario. • Todo el resto del tráfico está explícitamente denegado.	**1.3.2.a** Evalúe los estándares de configuración de los NSC para verificar que definen las restricciones del tráfico saliente desde el CDE de acuerdo con todos los elementos especificados en este requisito.	Este requisito tiene por objetivo prevenir que individuos malintencionados y componentes del sistema comprometidos dentro de la red de la entidad se comuniquen con un host externo no confiable. **Buenas prácticas** Todo el tráfico que sale del CDE, independientemente del destino, debe ser evaluado para asegurarse de que siguen reglas establecidas y autorizadas. Las conexiones deberían ser inspeccionadas para restringir el tráfico sólo a las comunicaciones autorizadas, por ejemplo, restringiendo a direcciones específicas de origen/destino y puertos, y bloqueando el contenido. **Ejemplos** Implementar una regla que deniega todo el tráfico entrante y saliente que no sea específicamente necesario -por ejemplo, utilizando una declaración explícita de "*Deny all*" o implícita de denegar después de permitir- ayuda a impedir agujeros involuntarios de tráfico no deseado y/o potencialmente dañino.
Objetivo del Enfoque Personalizado	**1.3.2.b** Evalúe las configuraciones de los NSC para verificar que el tráfico saliente desde el CDE está restringido de acuerdo con todos los elementos especificados en este requisito.	
El tráfico no autorizado no puede salir del CDE.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.3.3 Los NSC se implementan entre todas las redes inalámbricas y el CDE; esto es independientemente de que la red inalámbrica sea parte CDE o no, de manera que: • Todo el tráfico inalámbrico de las redes inalámbricas hacia el CDE es denegado de forma explícita. • Sólo se permite el tráfico inalámbrico al CDE que tenga un propósito de negocio autorizado.	**1.3.3** Evalúe los parámetros de configuración y los diagramas de red para verificar que los NSC son implementados entre todas las redes inalámbricas y el CDE, de acuerdo con todos los elementos especificados en este requisito.	La implementación y explotación conocida (o desconocida) de las tecnologías inalámbrica dentro de una red es una vía común para que los individuos malintencionados obtengan acceso a la red y a los datos del tarjetahabiente. Si se instala un dispositivo o una red inalámbrica sin el conocimiento de la entidad, personas malintencionadas podría entrar fácilmente y de forma "invisible" en la red. Si los NSC no restringen el acceso de las redes inalámbricas al CDE, personas malintencionadas que obtengan acceso no autorizado a la red inalámbrica pueden conectarse fácilmente al CDE y comprometer la información de las cuentas.
Objetivo del Enfoque Personalizado		
El tráfico no autorizado no puede atravesar los límites de la red entre cualquier red inalámbrica y el ambiente de red alámbricos en el CDE.		

Requisitos y Procedimientos de Prueba		Guía
1.4 Se controlan las conexiones de red entre las redes fiables y las que no lo son.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** La implementación de los NSC en cada conexión que entra y sale de las redes confiables permite a la entidad monitorear y controlar el acceso y minimiza las posibilidades de que individuos malintencionados logren ingresar a la red interna a través de una conexión no protegida. **Ejemplos** Una entidad podría implementar una DMZ, que es una parte de la red que gestiona las conexiones entre una red que no es confiable (para ver ejemplos de redes que no son fiables, consulte la descripción general del Requisito 1) y los servicios que la organización necesita mantener a disposición del público, tales como un servidor web. Tenga en cuenta que si la DMZ de una entidad procesa o transmite datos de cuentas (por ejemplo, un sitio web de comercio electrónico), también se considera parte del CDE o el CDE mismo.
1.4.1 Los NSC se implementan entre redes de confiables y no confiables.	**1.4.1.a** Evalúe los estándares de configuración y los diagramas de red para verificar que los CDE están definidos entre las redes confiables y no confiables.	
	1.4.1.b Evalúe las configuraciones de la red para verificar que los NSC están en implementados entre las redes confiables y no confiables, de acuerdo con los estándares de configuración documentadas y los diagramas de la red.	
Objetivo del Enfoque Personalizado		
El tráfico no autorizado no puede atravesar los límites de la red entre las redes confiables y no confiables.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.4.2 El tráfico entrante de redes que no son confiables a redes confiables está restringido a: • Las comunicaciones con componentes del sistema autorizados para proveer servicios de acceso público, protocolos y puertos. • Respuestas las comunicaciones previamente iniciadas por componentes del sistema en una red confiable, esto para protocolos con dicho comportamiento. • Todo el tráfico restante está denegado.	**1.4.2.** Evalúe la documentación del proveedor y las configuraciones de los NSC para verificar que el tráfico entrante de redes no confiables a redes confiables está restringido de acuerdo con todos los elementos especificados en este requisito.	Garantizar que el acceso público a un componente del sistema está específicamente autorizado reduce el riesgo de que los componentes del sistema queden expuestos innecesariamente a redes no confiables. **Buenas prácticas** Los componentes del sistema que proporcionan servicios de acceso público, tales como los servidores de correo electrónico, web y DNS, son los más vulnerables a las amenazas procedentes de redes no confiables. Lo ideal es que estos sistemas se instalen dentro de una red confiable especializada que esté orientada al público (por ejemplo, una DMZ) pero que esté separada de los sistemas internos más sensibles mediante un NSC, lo que ayuda a proteger el resto de la red en caso de que estos sistemas accesibles desde el exterior se vean comprometidos. Esta función pretende impedir que actores malintencionados accedan a la red interna de la organización desde Internet, o que utilicen servicios, protocolos o puertos de forma no autorizada. Cuando o donde esta función es proporcionada como una característica integrada de los NSC, la entidad debe asegurarse de que sus configuraciones no den como resultado la habilitación o un bypass de la misma. **Definiciones** Mantener el "estado" (o status) de cada conexión a una red significa que el NSC "sabe" si una aparente respuesta a una conexión anterior es una respuesta válida y autorizada (ya que el NSC conserva el estado de cada conexión) o si se trata de tráfico malintencionado que intenta engañar al NSC para que permita la conexión.
Objetivo del Enfoque Personalizado		
Solo el tráfico que está autorizado o que se genere como respuesta a un componente del sistema (esto solo para protocolos con dicho comportamiento) en la red confiable puede ingresar a una red confiable desde una red no confiable.		
Notas de Aplicabilidad		
La intención de este requisito es abordar las sesiones de comunicación entre redes confiables y no confiables, en lugar de las especificaciones de los protocolos. Este requisito no limita el uso de UDP u otros protocolos de red no orientados a conexión si el comportamiento estándar del estado de la conexión del protocolo es mantenido y bajo el control del NSC.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.4.3 Se implementan medidas *Antispoofing* para detectar y bloquear la entrada a la red confiable de direcciones IP origen falsas o suplantadas.	**1.4.3** Evalúe la documentación del fabricante y las configuraciones en los NSC para verificar que se implementen medidas *antispoofing* para detectar y bloquear la entrada la entrada a la red confiable de direcciones IP origen falsas o suplantadas.	El filtrado de paquetes que ingresan a la red confiable ayuda, entre otras cosas, a garantizar que los paquetes no sean "falsificados" y que aparenten provenir de la propia red interna de una organización. Por ejemplo, las medidas *antispoofing* impiden que las direcciones internas que se originan en Internet pasen a la DMZ. **Buenas prácticas** Los productos generalmente vienen con un conjunto medidas *antispoofing* predeterminado y es posible que no se puedan configurar. Las entidades deben consultar la documentación del proveedor para obtener más información. **Ejemplos** Normalmente, un paquete contiene la dirección IP origen de la computadora que lo envió para que otras computadoras en la red sepan dónde se originó el paquete. Personas malintencionadas a menudo intentarán suplantar (o imitar) la dirección IP de envío para engañar al sistema de destino haciéndole creer que el paquete proviene de una fuente confiable.
Objetivo del Enfoque Personalizado		
Los paquetes con direcciones IP origen falsas o suplantadas no pueden ingresar a una red confiable.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.4.4 Los componentes del sistema que almacenan datos de titulares de tarjetas no son accesibles directamente desde redes no confiables.	**1.4.4.a** Evalúe los diagramas de flujo y de red para verificar que esté documentado que los componentes del sistema que almacenan datos de los titulares de tarjetas no puedan accederse directamente desde redes no confiables.	Los datos de los titulares de tarjeta a los que se puede acceder directamente desde una red no confiable, por ejemplo, debido a que están almacenados en un sistema dentro de la DMZ o en un servicio de base de datos en la nube, son más fáciles de acceder para un atacante externo porque hay menos capas defensivas que penetrar. El uso de los NSC para asegurar que los componentes del sistema que almacenan datos de titulares de tarjetas (como una base de datos o un archivo) sólo pueden ser accedidos directamente desde redes confiables, lo que puede prevenir que el tráfico de red no autorizado alcance el componente del sistema que almacena datos de titulares de tarjetas.
Objetivo del Enfoque Personalizado	**1.4.4.b** Evalúe las configuraciones de los NSC para verificar que se implementen controles de manera que los componentes del sistema que almacenan datos de titulares de tarjetas no sean directamente accesibles desde redes no confiables.	
No se puede acceder a los datos de los titulares de tarjetas almacenados desde redes no confiables.		
Notas de Aplicabilidad		
Este requisito no se aplica al almacenamiento de datos de cuentas en memoria volátil, pero sí se aplica cuando la memoria se trata como almacenamiento persistente (por ejemplo, disco RAM). Los datos del tarjetahabiente sólo pueden almacenarse en la memoria volátil durante el tiempo necesario para soportar el proceso de negocio asociado (por ejemplo, hasta la finalización transacción relacionada con tarjeta de pago).		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Restringir la divulgación de las direcciones IP internas, privadas y locales es útil para impedir que hackers obtengan esas direcciones IP y utilicen esa información para acceder a la red. **Buenas prácticas** Los métodos utilizados para cumplir con el propósito de este requisito pueden variar, dependiendo de la tecnología de red específica que se utilice. Por ejemplo, los controles utilizados para cumplir este requisito pueden ser distintos para las redes IPv4 que para las redes IPv6. **Ejemplos** Los métodos para ocultar el direccionamiento IP pueden incluir, entre otros, los siguientes • Traducción de Direcciones IP de Red IPv4 (NAT). • Implementación de componentes del sistema detrás de servidores proxy/NSC. • Eliminación o filtrado de los mensajes de enrutamiento para las redes internas que utilizan direcciones registradas. • Uso interno del RFC 1918 (IPv4) o uso de la extensión de privacidad IPv6 (RFC 4941) al iniciar sesiones salientes a Internet.
1.4.5 La divulgación de las direcciones IP internas y la información de enrutamiento se limita sólo a las partes autorizadas.	**1.4.5.a** Evalúe las configuraciones de los NSC para verificar que la divulgación de las direcciones IP internas y la información de enrutamiento se limita sólo a las partes autorizadas.	
	1.4.5.b Entreviste al personal y Evalúe la documentación para verificar que se implementen los controles de manera que la divulgación de las direcciones IP internas y la información de enrutamiento se limite sólo a las partes autorizadas.	
Objetivo del Enfoque Personalizado		
La información interna de red está protegida contra la divulgación no autorizada.		

Requisitos y Procedimientos de Prueba		Guía
1.5 Se mitigan los riesgos para el CDE desde dispositivos informáticos que pueden conectarse tanto a redes no confiables como al CDE.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
1.5.1 Los controles de seguridad se implementan en cualquier dispositivo informático, incluyendo los dispositivos propiedad de la empresa y de los empleados, que se conectan tanto a redes no confiables (incluida Internet) como al CDE manera siguiente: • Se definen los parámetros de configuración específicos para impedir que se introduzcan amenazas en la red de la entidad. • Los controles de seguridad se están ejecutando activamente. • Los usuarios de los dispositivos informáticos no pueden alterar los controles de seguridad a menos que estén específicamente documentados y autorizados por el nivel gerencial, caso por caso, durante un período limitado.	**1.5.1.a** Evalúe las políticas y estándares de configuración y entreviste al personal para verificar que los controles de seguridad de los dispositivos informáticos que se conectan a redes no fiables y al CDE estén implementados de acuerdo con todos los elementos descritos en este requisito. **1.5.1.b** Evalúe los parámetros de configuración en los dispositivos informáticos que se conectan a redes no confiables y al CDE para verificar que los parámetros o configuraciones se implementen de acuerdo con todos los elementos especificados en este requisito.	Los dispositivos informáticos que pueden conectarse a Internet desde fuera del entorno corporativo, por ejemplo, computadoras de escritorio, portátiles, tabletas, teléfonos inteligentes y otros dispositivos informáticos móviles utilizados por los empleados, son más vulnerables a las amenazas basadas en Internet. El uso de controles de seguridad, tales como controles basados en el host (por ejemplo, software de *firewalls* personal o soluciones de protección tipo *end point*), controles de seguridad basados en la red (por ejemplo, *firewalls*, redes basadas en inspecciones heurísticas y simulación de malware) o hardware, ayuda a proteger los dispositivos desde los ataques basados en Internet, los cuales podrían utilizar los dispositivos para obtener acceso a los sistemas y datos de la organización cuando el dispositivo se vuelva a conectar a la red.
Objetivo del Enfoque Personalizado		
Los dispositivos que se conectan a entornos no confiables y que también se conectan al CDE no pueden presentar o introducir amenazas al CDE de la entidad.		*(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Estos controles de seguridad pueden desactivarse temporalmente solo si existe una necesidad técnica legítima, según lo autorizado por el nivel gerencial caso por caso. Se requiere de una autorización formal para desactivar estos controles de seguridad para y bajo un propósito específico. También puede ser necesario implementar medidas de seguridad adicionales durante el período en el cual estos controles seguridad estén desactivados. Este requisito aplica a los dispositivos informáticos que sean propiedad tanto de la entidad como de los empleados. Los sistemas que no pueden ser administrados por políticas corporativas introducen debilidades y brindan oportunidades para que personas malintencionadas pueden explotarlas y/o aprovecharlas.		**Buenas prácticas** Los parámetros de configuración específicos los determina la entidad y deben ser coherentes con sus políticas y procedimientos de seguridad de red. Cuando existe una necesidad legítima de deshabilitar temporalmente los controles de seguridad en un dispositivo propiedad de la empresa o del empleado que se conecta tanto a una red que no es confiable como al CDE, por ejemplo, para soportar una actividad de mantenimiento específica o la investigación de un problema técnico, el motivo para desarrollar tal acción debe ser informado y aprobado por un gerente autorizado. Cualquier desactivación o alteración de estos controles de seguridad, incluso en los dispositivos de los propios administradores, solo podrá ser realizado por personal autorizado. Se reconoce que los administradores tienen privilegios que podrían permitirles deshabilitar los controles de seguridad en sus propias computadoras, pero deben existir mecanismos de alerta cuando dichos controles estén deshabilitados y se debe realizar seguimiento para garantizar que se aplican los procedimientos de seguridad de red. **Ejemplos** Las prácticas incluyen prohibir Split-tunneling de VPN para dispositivos móviles propiedad de los empleados o de la entidad y se requiere que dichos dispositivos se inicien dentro de una VPN.

Requisito 2: Aplicar Configuraciones Seguras a Todos los Componentes del Sistema

Secciones
2.1 Se definen y comprenden los procesos y mecanismos para aplicar configuraciones seguras a todos los componentes del sistema.
2.2 Los componentes del sistema se configuran y administran de forma segura.
2.3 Los entornos inalámbricos se configuran y gestionan de forma segura.

Descripción
Personas malintencionadas, tanto externas como internas de una entidad, a menudo utilizan contraseñas predeterminadas y otras configuraciones predeterminadas del proveedor para comprometer los sistemas. Estas contraseñas y configuraciones son bien conocidas y se determinan fácilmente a través de información pública.
La aplicación de configuraciones seguras a los componentes del sistema reduce los medios disponibles para que un atacante comprometa el sistema. Cambiar las contraseñas predeterminadas, eliminar software, funciones y cuentas innecesarias, y deshabilitar o eliminar servicios innecesarios ayudan a reducir los potenciales ataques.
Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
2.1 Se definen y comprenden los procesos y mecanismos para aplicar configuraciones seguras a todos los componentes del sistema.		
Requisitos del Enfoque Definido **2.1.1** Todas las políticas de seguridad y los procedimientos operativos que se identifican en el Requisito 2 están: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la vigilancia en el cumplimiento de las actividades del Requisito 2 están definidos y son realizados por el personal afectado. Todas las actividades de apoyo son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.	**Procedimientos de Prueba del Enfoque Definido** **2.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 2 se gestionen de acuerdo con todos los elementos especificados en este requisito.	**Propósito** El Requisito 2.1.1 trata sobre la gestión y el mantenimiento eficaz de las diversas políticas y procedimientos especificados en el Requisito 2. Si bien es importante definir las políticas o procedimientos específicos indicados en el Requisito 2, es igualmente importante asegurarse de que estén debidamente documentados, mantenidos y difundidos. **Buenas prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos empresariales. Por esta razón, considere actualizar estos documentos lo antes posible después de que ocurra un cambio y no solo en un ciclo periódico. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que las actividades críticas no se realicen. **Buenas prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
2.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 2 son documentadas, asignadas y comprendidas.	**2.1.2.a** Evalúe la documentación para verificar que las descripciones de las funciones y las responsabilidades para realizar las actividades del Requisito 2 están documentadas y asignadas.	
	2.1.2.b Entreviste al personal responsable de realizar las actividades del Requisito 2 para verificar que los roles y responsabilidades se asignan y son documentadas y entendidas.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 2. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
2.2 Los componentes del sistema se configuran y administran de forma segura.		
Requisitos del Enfoque Definido **2.2.1** Los estándares de configuración se desarrollan, implementan y mantienen para: • Cubrir todos los componentes del sistema. • Cubrir todas las vulnerabilidades de seguridad conocidas. • Brindar coherencia con el estándar de *hardening* del sistema aceptadas por el sector o con las recomendaciones de *hardening* del proveedor. • Ser actualizadas a medida que se identifican nuevos problemas de vulnerabilidad, como se define en el requisito 6.3.1. • Ser aplicadas cuando los nuevos sistemas sean configurados y verificadas como establecidas antes o inmediatamente después de que un componente del sistema se conecte a un entorno de producción. **Objetivo del Enfoque Personalizado** Todos los componentes del sistema están configurados de forma segura y coherente y de acuerdo con el estándar de *hardening* aceptados por el sector o las recomendaciones del proveedor.	**Procedimientos de Prueba del Enfoque Definido** **2.2.1.a** Evalúe los estándares de configuración del sistema para verificar que definen procesos que incluyen todos los elementos descritos en este requisito. **2.2.1.b** Evalúe las políticas y procedimientos y entreviste al personal para verificar que los estándares de configuración del sistema se actualizan a medida que se identifican nuevos problemas de vulnerabilidad, como se define en el Requisito 6.3.1. **2.2.1.c** Evalúe los ajustes de configuración y entreviste al personal para verificar que los estándares de configuración del sistema se aplican cuando se configuran nuevos sistemas y se verifica que están instalados antes o inmediatamente después de que un componente del sistema se conecte a un entorno de producción.	**Propósito** Existen debilidades conocidas en muchos sistemas operativos, bases de datos, dispositivos de red, softwares, aplicaciones, imágenes de contenedores y otros dispositivos utilizados por una entidad o dentro de su entorno. También hay formas conocidas de configurar esos componentes del sistema para solucionar las vulnerabilidades de seguridad. Corregir las vulnerabilidades de seguridad reduce las oportunidades disponibles para un atacante. Mediante el desarrollo de estándares, las entidades se aseguran de que los componentes de sus sistemas se configuren de forma coherente y segura, y abordan la protección de dispositivos para los cuales el *hardening* más estricto de las medidas puede ser más difícil. **Buenas prácticas** Mantenerse al día con las orientaciones actuales del sector ayudará a la entidad a mantener configuraciones seguras. Los controles específicos que se apliquen a un sistema variarán y deberán ser apropiados para el tipo y la función del sistema. Muchas organizaciones de seguridad han establecido directrices y recomendaciones de *hardening* del sistema, con lo que aconsejan cómo corregir las debilidades comunes y conocidas. **Información adicional** Las fuentes de información sobre los estándares de configuración son, entre otros, los siguientes: Centro de Seguridad en Internet (CIS), Organización Internacional de Estandarización (ISO), Instituto Nacional de Estándares y Tecnología (NIST), Cloud Security Alliance, y proveedores de productos.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
2.2.2 Las cuentas predeterminadas del proveedor se gestionan de la siguiente manera: • Si se utilizan las cuentas predeterminadas del proveedor, la contraseña predeterminada se cambia según el requisito 8.3.6. • Si no se van a utilizar las cuentas predeterminadas del proveedor, la cuenta se elimina o se desactiva.	**2.2.2.a** Evalúe los estándares de configuración del sistema para comprobar que incluyen la gestión de las cuentas predeterminadas del proveedor de acuerdo con todos los elementos especificados en este requisito. **2.2.2.b** Evalúe la documentación del proveedor y observe al administrador del sistema iniciando sesión utilizando las cuentas predeterminadas del proveedor para verificar que las cuentas se implementan de acuerdo con todos los elementos especificados en este requisito. **2.2.2.c** Evalúe los archivos de configuración y entreviste al personal para verificar que todas las cuentas predeterminadas del proveedor que no se utilizarán sean eliminadas o deshabilitadas.	Personas malintencionadas suelen utilizar los nombres de cuentas y contraseñas predeterminadas del proveedor para poner en peligro los sistemas operativos, las aplicaciones y los sistemas en los que están instalados. Debido a que estas configuraciones predeterminadas a menudo se publican y son bien conocidas, su cambio hará que los sistemas sean menos vulnerables a los ataques. **Buenas prácticas** Deben identificarse todas las cuentas predeterminadas de los proveedores, y entenderse su propósito y uso. Es importante establecer controles para cuentas de aplicaciones y sistemas, incluyendo las utilizadas para desplegar y mantener los servicios en la nube, de modo que no utilicen contraseñas predeterminadas y que no puedan ser utilizadas por personas no autorizadas. Cuando no se pretenda utilizar una cuenta predeterminada, el cambio de la contraseña predeterminada por una contraseña única que cumpla con el Requisito 8.3.6 PCI DSS, la eliminación de cualquier acceso a la cuenta predeterminada y la posterior desactivación de la cuenta, impedirán que personas malintencionadas vuelvan a activar la cuenta y obtengan acceso con la contraseña predeterminada. Se recomienda utilizar una red de ensayo aislada para instalar y configurar nuevos sistemas, y también puede utilizarse para confirmar que no se han introducido credenciales predeterminadas en los entornos de producción. (continúa en la página siguiente)
Objetivo del Enfoque Personalizado		
No se puede acceder a los componentes del sistema utilizando contraseñas predeterminadas.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Esto se aplica a TODAS las cuentas y contraseñas predeterminadas del proveedor, incluidas, entre otras, las utilizadas por los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de punto de venta (POS), las aplicaciones de pago y los valores predeterminados del Protocolo Simple de Administración de Red (SNMP). Este requisito también se aplica cuando un componente del sistema no está instalado en el entorno de una entidad, por ejemplo, el software y las aplicaciones que forman parte del CDE y a las que se ingresa a través de un servicio de suscripción en la nube.		**Ejemplos** Los valores predeterminados que se deben tener en cuenta incluyen los identificadores de usuario, las contraseñas y otras credenciales de autenticación utilizadas habitualmente por los proveedores en sus productos.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
2.2.3 Las funciones principales que requieren distintos niveles de seguridad se administran de la siguiente manera: • Solo existe una función principal en un componente del sistema, **O** • Las funciones principales con distintos niveles de seguridad que existen en el mismo componente del sistema están aisladas entre sí, **O** • Las funciones principales con distintos niveles de seguridad en el mismo componente del sistema están todas aseguradas al nivel requerido por la función que requiera un nivel mayor de seguridad.	**2.2.3.a** Evalúe los estándares de configuración del sistema para verificar que incluyan la gestión de funciones principales que requieran distintos niveles de seguridad como se especifica en este requisito.	**Propósito** Los sistemas que contienen una combinación de servicios, protocolos y «demonios» para su función principal tendrán un perfil de seguridad apropiado que permita que esa función opere eficientemente. Por ejemplo, los sistemas que necesitan estar conectados directamente a Internet tendrían un perfil particular, como un servidor DNS, un servidor web o un servidor de comercio electrónico. A la inversa, otros componentes del sistema pueden operar una función principal que involucra un conjunto distinto de servicios, protocolos y «demonios» que realizan funciones que la entidad prefiere no exponer a internet". Este requisito tiene como objetivo garantizar que las distintas funciones no afecten los perfiles de seguridad de otros servicios de una manera que pueda hacerlos operar a un nivel de seguridad mayor o menor. **Buenas prácticas** Lo ideal es que cada función se ubique en componentes distintos del sistema. Esto se puede lograr implementando solo una función principal en cada componente del sistema. Otra opción es aislar las funciones principales en el mismo componente del sistema que tiene distintos niveles de seguridad, por ejemplo, aislar los servidores web (que deben estar conectados directamente a Internet) de los servidores de aplicaciones y bases de datos. *(continúa en la página siguiente)*
	2.2.3.b Evalúe las configuraciones del sistema para verificar que las funciones principales que requieren distintos niveles de seguridad se administren de acuerdo con una de las formas especificadas en este requisito.	
	2.2.3.c Cuando se utilizan tecnologías de virtualización, Evalúe las configuraciones del sistema para verificar que aquellas funciones que requieran distintos niveles de seguridad se gestionen en una de las siguientes maneras: • Las funciones con distintas necesidades de seguridad no coexisten en el mismo componente del sistema. • Las funciones con distintas necesidades de seguridad que existen en el mismo componente del sistema están aisladas entre sí. • Las funciones con distintas necesidades de seguridad en el mismo componente del sistema están todas aseguradas al nivel requerido por aquella función con el mayor requerimiento de seguridad.	
Objetivo del Enfoque Personalizado		
Las funciones principales con necesidades de seguridad más bajas no pueden afectar la seguridad de las funciones principales con necesidades de seguridad más elevadas dentro del mismo componente del sistema.		

Requisitos y Procedimientos de Prueba		Guía
		Si un componente del sistema contiene funciones principales que necesitan distintos niveles de seguridad, una tercera opción es implementar controles adicionales para garantizar que el nivel de seguridad resultante de las funciones principales con necesidades de seguridad más elevadas no se reduzca por la presencia funciones principales que requieran menos seguridad. Además, las funciones con un nivel de seguridad más bajo deben aislarse y/o protegerse para garantizar que no puedan acceder o afectar los recursos de otra función del sistema, y que no introduzcan deficiencias de seguridad en otras funciones dentro del mismo servidor. Las funciones de diferentes niveles de seguridad pueden aislarse mediante controles físicos o lógicos. Por ejemplo, un sistema de base de datos no debería albergar también servicios web a menos que se utilicen controles como tecnologías de virtualización para aislar y contener las funciones en sub-sistemas separados. Otro ejemplo es el uso de instancias virtuales o la provisión de acceso a memoria especializada por cada función del sistema. Cuando se utilizan tecnologías de virtualización, los niveles de seguridad deben identificarse y administrarse para cada componente virtual. Algunos ejemplos de consideraciones a tomar para entornos virtualizados incluyen: • La función de cada aplicación, contenedor o instancia de servidor virtual. • Cómo se almacenan y protegen las máquinas virtuales (VM) o los contenedores.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Los servicios y funciones innecesarios pueden brindar oportunidades adicionales para que individuos malintencionados obtengan acceso a un sistema. Al eliminar o deshabilitar todos los servicios, protocolos, «demonios» y funciones innecesarias, las organizaciones pueden concentrarse en proteger las funciones que se requieren y reducir el riesgo de que se exploten funciones desconocidas o innecesarias. **Buenas prácticas** Hay muchos protocolos que podrían habilitarse de forma predeterminada y que son comúnmente utilizados por personas malintencionadas para comprometer una red. Deshabilitar o eliminar todos los servicios, funciones y protocolos que no se utilizan minimiza la superficie de ataque potencial, por ejemplo, al eliminar o deshabilitar un servidor web o FTP no utilizado. **Ejemplos** Las funciones innecesarias pueden incluir, entre otros, scripts, controladores, características, sub-sistemas, sistemas de archivos, interfaces (USB y Bluetooth) y servidores web innecesarios.
2.2.4 Solo se habilitan los servicios, protocolos, «demonios» y funciones necesarias, y se eliminan o deshabilitan todas las funciones innecesarias.	**2.2.4.a** Evalúe los estándares de configuración del sistema para verificar que los servicios, protocolos y «demonios» requeridos por el sistema estén identificados y documentados.	
	2.2.4.b Evalúe las configuraciones del sistema para verificar lo siguiente: • Todas las funciones innecesarias se eliminan o desactivan. • Solo se habilitan las funciones requeridas como aparece documentado en los estándares de configuración.	
Objetivo del Enfoque Personalizado		
Los componentes del sistema no pueden verse comprometidos explotando funciones innecesarias presentes en el componente del sistema.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Asegurarse de que todos los servicios, protocolos y «demonios» inseguros estén adecuadamente protegidos con características de seguridad apropiadas que dificulten a las personas malintencionadas explotar los puntos comunes de debilidades dentro de una red. **Buenas prácticas** Habilitar las funciones de seguridad antes de que se implementen los nuevos componentes del sistema impedirá que se introduzcan configuraciones inseguras en el entorno. Algunas soluciones de proveedores pueden proporcionar funciones de seguridad adicionales para ayudar a proteger un proceso inseguro. **Información adicional** Para obtener orientación sobre servicios, protocolos o «demonios» que se consideran inseguros, consulte los Estándares y las guías de la industria (por ejemplo, según lo publicado por NIST, ENISA y OWASP).
2.2.5 Si existen servicios, protocolos o «demonios» inseguros: • La justificación de negocio está documentada. • Se documentan e implementan características de seguridad adicionales que reducen el riesgo de utilizar servicios, protocolos o "demonios" inseguros.	**2.2.5.a** Si existen servicios, protocolos o "demonios" inseguros, Evalúe los estándares de configuración del sistema y entreviste al personal para verificar que estén administrados e implementados de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado	**2.2.5.b** Si existen servicios, protocolos o "demonios" inseguros, Evalúe los valores de configuración para verificar que se hayan implementado funciones de seguridad adicionales para reducir el riesgo de utilizar protocolos, "demonios" y servicios inseguros.	
Los componentes del sistema no pueden ser comprometidos explotando servicios, protocolos o "demonios" inseguros.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
2.2.6 Los parámetros de seguridad del sistema están configurados para impedir su uso indebido.	**2.2.6.a** Evalúe los estándares de configuración del sistema para comprobar que incluyen la configuración de los parámetros de seguridad del sistema a fin de impedir su uso indebido.	**Propósito** La configuración correcta de los parámetros de seguridad proporcionados en los componentes del sistema aprovecha las capacidades del componente del sistema para frustrar los ataques malintencionados. **Buenas prácticas** Los estándares de configuración del sistema y los procesos relacionados deben abordar específicamente los ajustes y parámetros de seguridad que tienen implicaciones de seguridad conocidas para cada tipo de sistema en uso. Para que los sistemas se configuren de forma segura, el personal responsable de la configuración y/o administración de los sistemas debe conocer los parámetros y ajustes de seguridad específicos que se aplican al sistema. Debe considerarse también la configuración segura de los parámetros utilizados para acceder a los portales en la nube. **Información adicional** Consulte la documentación del proveedor y las referencias del sector indicadas en el Requisito 2.2.1 para obtener información sobre los parámetros de seguridad aplicables a cada tipo de sistema.
	2.2.6.b Entreviste a los administradores del sistema y/o gerentes de seguridad para verificar que tienen conocimiento de la configuración de los parámetros de seguridad comunes para los componentes del sistema.	
Objetivo del Enfoque Personalizado	**2.2.6.c** Evalúe la configuración del sistema para verificar que los parámetros comunes de seguridad están configurados adecuadamente y de acuerdo con los estándares de configuración del sistema.	
Los componentes del sistema no pueden ser comprometidos debido a una configuración incorrecta de los parámetros de seguridad.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
2.2.7 Todo el acceso administrativo sin consola está cifrado utilizando criptografía sólida.	**2.2.7.a** Evalúe los estándares de configuración del sistema para verificar que incluyan el cifrado de todos los accesos administrativos sin consola mediante una criptografía sólida.	**Propósito** Si la administración sin-consola (incluyendo la remota) no utiliza comunicaciones cifradas, los factores de autorización administrativa (tales como IDs y contraseñas) pueden ser revelados a espías. Un individuo malintencionado podría utilizar esta información para acceder a la red, convertirse en administrador y robar datos. **Buenas prácticas** Cualquiera que sea el protocolo de seguridad utilizado, este debe ser configurado para utilizar sólo versiones y configuraciones seguras a fin de impedir el uso de conexiones inseguras: por ejemplo, usando sólo certificados de confianza, brindando apoyo sólo con encriptación sólida, y no respaldando auxiliares de protocolos o métodos más débiles e inseguros. **Ejemplos** Los protocolos de texto en claro (como HTTP, telnet, etc.) no cifran el tráfico ni los detalles de inicio de sesión, lo que facilita que los espías intercepten esta información. El acceso sin consola puede ser facilitado por tecnologías que brindan acceso alternativo a los sistemas, incluyendo, entre otros, fuera de banda (OOB), gestión de luces apagadas (LOM), Interfaz de Gestión de Plataforma Inteligente (IPMI) y teclado, video, conmutadores de mouse (KVM) con capacidades remotas. Estas y otras tecnologías y métodos de acceso sin consola deben protegerse con una criptografía sólida. **Información adicional** Consulte los estándares y mejores prácticas de la industria, como *NIST SP 800-52 y SP 800-57.*
	2.2.7.b Observe cómo un administrador inicia sesión en los componentes del sistema y examine las configuraciones del sistema para verificar que el acceso administrativo sin consola se administre de acuerdo con este requisito.	
	2.2.7.c Evalúe la configuración de los componentes del sistema y los servicios de autenticación para verificar que los servicios de inicio de sesión remota inseguros no estén disponibles para el acceso administrativo sin consola.	
	2.2.7.d Evalúe la documentación del proveedor y entreviste al personal para verificar que se implemente una criptografía sólida para la tecnología en uso de acuerdo con las mejores prácticas de la industria y / o las recomendaciones del proveedor.	
Objetivo del Enfoque Personalizado Los factores de autorización administrativa en texto claro no se pueden leer ni interceptar desde ninguna transmisión de red.		
Notas de Aplicabilidad Esto incluye el acceso administrativo a través de interfaces basadas en navegador e interfaces de programación de aplicaciones (API).		

Requisitos y Procedimientos de Prueba		Guía
2.3 Los entornos inalámbricos se configuran y administran de forma segura.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
2.3.1 Para entornos inalámbricos conectados al CDE o que transmiten datos de la cuenta, todos los valores predeterminados de los proveedores inalámbricos se cambian en la instalación o se confirma que son seguros, incluidos, entre otros: • Claves de cifrado inalámbricas predeterminadas. • Contraseñas o puntos de acceso inalámbricos. • Valores predeterminados de SNMP. • Cualquier otro proveedor inalámbrico predeterminado relacionado con la seguridad.	**2.3.1.a** Evalúe las políticas y los procedimientos y entreviste al personal responsable para verificar que los procesos estén definidos para los valores predeterminados de los proveedores inalámbricos, sea para cambiarlos en el momento de la instalación o para confirmar que son seguros de acuerdo con todos los elementos de este requisito.	Si las redes inalámbricas no se implementan con suficientes configuraciones de seguridad (incluido el cambio de la configuración predeterminada), los rastreadores inalámbricos pueden espiar el tráfico, capturar fácilmente datos y contraseñas, entrar y atacar fácilmente la red. **Buenas prácticas** Las contraseñas inalámbricas deben construirse de manera que sean resistentes a los ataques de fuerza bruta fuera de línea.
	2.3.1.b Evalúe la documentación del proveedor y observe cómo un administrador del sistema inicia sesión en los dispositivos inalámbricos para verificar que: • No se utilizan los valores predeterminados de SNMP. • No se utilizan contraseñas/frases de contraseña predeterminadas en los puntos de acceso.	
Objetivo del Enfoque Personalizado No se puede acceder a las redes inalámbricas utilizando contraseñas predeterminadas del proveedor o configuraciones predeterminadas.	**2.3.1.c** Evalúe la documentación del proveedor y los ajustes de configuración inalámbrica para verificar que se hayan cambiado otros valores predeterminados de proveedores inalámbricos relacionados con la seguridad, si corresponde.	
Notas de Aplicabilidad Esto incluye, pero no se limita a, las claves de encriptación inalámbrica predeterminadas, las contraseñas de los puntos de acceso inalámbricos, los valores predeterminados de SNMP y cualquier otro valor predeterminado del proveedor inalámbrico relacionado con la seguridad.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Cambiar las claves de cifrado de redes inalámbricas cada vez que alguien con conocimiento de la clave abandona la organización o se traslada a un puesto para el cual ya no requiere la clave, ayuda a mantener el conocimiento de las claves limitado solamente a aquellos que lo requieran por motivos de negocios. Además, cambiar las claves de cifrado de redes inalámbricas cada vez que se sospeche o se sepa que una clave está comprometida, hacen las redes inalámbricas más resistentes a los riesgos. **Buenas prácticas** Este objetivo puede cumplirse de varias formas, incluyendo cambios periódicos de las claves, cambiando las claves a través de un proceso definido de "unión-mudanza-desconexión" (JML), implementando controles técnicos adicionales y no utilizando claves fijas pre-compartidas. Además, cualquier clave que se sepa o se sospeche que está comprometida debe gestionarse de acuerdo con el plan de respuesta a incidentes de la entidad en el Requisito 12.10.1.
2.3.2 Para los entornos inalámbricos conectados al CDE o que transmitan datos de cuentas, las claves cifradas inalámbricas se cambian como sigue: • Siempre que el personal con conocimiento de la clave deje la empresa o la función para la que era necesario el conocimiento. • Siempre que se sospeche o se sepa que una clave está comprometida.	**2.3.2** Entreviste al personal responsable y examine la documentación de gestión de claves para verificar que las claves de cifrado inalámbricas se cambian de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado		
El conocimiento de las claves cifradas inalámbricas no puede permitir el acceso no autorizado a las redes inalámbricas.		

Proteger los Datos del Tarjetahabiente

Requisito 3: Proteger los Datos de Tarjetahabientes Almacenados

Secciones	
3.1	Se definen y comprenden los procesos y los mecanismos para proteger los datos de cuentas almacenados.
3.2	El almacenamiento de los datos de cuentas se reduce al mínimo.
3.3	Los datos confidenciales de autenticación (SAD) no se almacenan después de su autorización.
3.4	El acceso a la visualización del PAN completo y la capacidad de copiar los datos de titulares de tarjetas están restringidos.
3.5	El número de cuenta principal (PAN) está protegido dondequiera que se almacene.
3.6	Las claves criptográficas utilizadas para proteger los datos almacenados del tarjetahabiente están protegidos.
3.7	Cuando se utiliza la criptografía para proteger los datos almacenados del tarjetahabiente se definen e implementan procesos y procedimientos de gestión de claves que cubren todos los aspectos del ciclo de vida de las mismas.

Descripción

Los métodos de protección como el cifrado, el truncamiento, el enmascaramiento y el *hash* son componentes críticos de la protección de los datos de cuentas. Si un intruso elude otros controles de seguridad y logra tener acceso a los datos cuentas cifrados, esos datos son ilegibles sin las claves criptográficas adecuadas y son inutilizables. Otros métodos eficientes de protección de datos almacenados también deben considerarse como oportunidades potenciales de mitigación de riesgos. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar los datos cuentas a menos que sea necesario, truncar los datos del titular de la tarjeta si no se necesitan los datos PAN completos, y no enviar aquellos datos PAN no-protegidos al usuario final utilizando tecnologías de mensajería como el correo electrónico y la mensajería instantánea.

Si los datos de la cuenta se encuentran en una memoria no persistente (por ejemplo, RAM, memoria volátil), no es necesario cifrarlos. Sin embargo, deben establecerse controles adecuados para garantizar que la memoria mantiene un estado no persistente. Los datos deben ser eliminados de la memoria volátil una vez que el propósito del negocio (por ejemplo, la transacción asociada) se haya completado. En caso de que el almacenamiento de datos se vuelva persistente, se aplicarán todos los requisitos de PCI DSS aplicables, incluidos el cifrado de datos almacenados.

El requisito 3 se aplica a la protección de los datos almacenados de las cuentas, a menos que se mencione específicamente en un requisito individual.

Consulte el Anexo G para conocer las definiciones de "criptografía sólida" y otros términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
3.1 Se definen y comprenden los procesos y mecanismos para proteger los datos de cuentas almacenados.		
Requisitos del Enfoque Definido **3.1.1** Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 3 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la vigilancia en el cumplimiento con las actividades dentro del Requisito 3 están definidos y cumplidos por el personal afectado. Todas las actividades de apoyo son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.	**Procedimientos de Prueba del Enfoque Definido** **3.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 3 se gestionen de acuerdo con todos los elementos especificados en este requisito.	**Propósito** El Requisito 3.1.1 trata sobre la gestión y el mantenimiento eficiente de las diversas políticas y procedimientos especificados en el Requisito 3. Si bien es importante definir las políticas o procedimientos específicos indicados en el Requisito 3, es igualmente importante asegurarse de que estén debidamente documentados, mantenidos y difundidos. **Buenas prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos empresariales. Por esta razón, considere actualizar estos documentos lo más pronto posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que las actividades críticas no se desarrollen. **Buenas prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
3.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 3 están documentados, asignados y comprendidos.	**3.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y responsabilidades que realizan las actividades del Requisito 3 estén documentadas y asignadas.	
	3.1.2.b Entreviste al personal responsable de desarrollar las actividades del Requisito 3 para verificar que los roles y responsabilidades se asignen según se documenten y sean entendidos.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 3. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
3.2 El almacenamiento de los datos de la cuenta se mantiene al mínimo.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
3.2.1 El almacenamiento de datos de cuentas se mantiene al mínimo mediante la implementación de políticas y procedimientos de retención y eliminación de datos que incluyan al menos lo siguiente: • Cubren todas las ubicaciones donde hay datos de cuentas almacenados. Cubren todo dato de autenticación confidencial (SAD) almacenado antes de completar la autorización. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; refiérase a las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.* • Limitar la cantidad de datos almacenados y su tiempo de retención a lo requerido por los requisitos legales o reglamentarios y/o de negocios. • Requisitos de retención específicos para los datos de cuentas almacenados que definen la duración del período de retención e incluyen una justificación de negocio documentada. • Procesos para el borrado seguro o para hacer que los datos del tarjetahabiente sean irrecuperables cuando ya no se necesitan según la política de retención. • Un proceso para verificar, al menos una vez cada tres meses, que los datos de cuentas almacenados que excedan el período de retención definido se han eliminado de forma segura o se han vuelto irrecuperables.	**3.2.1.a** Evalúe las políticas y procedimientos de retención y eliminación de datos, y entreviste al personal para verificar que los procesos estén definidos para incluir todos los elementos especificados en este requisito. **3.2.1.b** Evalúe los archivos y registros de los componentes del sistema en los que se almacenan los datos de cuentas, para verificar que la cantidad de datos almacenados y el tiempo de retención no excedan los requisitos definidos en la política de retención de datos. **3.2.1.c** Observe los mecanismos utilizados para hacer que los datos de cuentas sean irrecuperables para verificar que no se puedan recuperar.	**Propósito** Una política formal de retención de datos identifica qué datos deben conservarse, por cuánto tiempo, y dónde residen esos datos, de manera que puedan destruirse o eliminarse de forma segura tan pronto como ya no se necesiten. Los únicos datos de la cuenta que podrían almacenarse después de la autorización son el número de cuenta principal o PAN (que se vuelve ilegible), la fecha de caducidad, el nombre del titular de la tarjeta y el código de servicio. El almacenamiento de datos de SAD antes de finalizado el proceso de autorización también es parte de la política de retención y eliminación de datos; de manera que se mantenga al mínimo el almacenamiento de esos datos confidenciales y sólo se conserven durante un período de tiempo definido. **Buenas prácticas** Al identificar las ubicaciones de los datos de cuenta almacenados, considere todos los procesos y el personal con acceso a los datos, ya que los datos podrían haberse movido y almacenado en ubicaciones diferentes a las que se definieron originalmente. Las ubicaciones de almacenamiento que a menudo se pasan por alto incluyen sistemas de apoyo y archivo, dispositivos de almacenamiento de datos extraíbles, medios en papel y grabaciones de audio. Para definir los requisitos de retención apropiados, la entidad debe comprender primeramente sus propias necesidades de negocios, así como las obligaciones legales o reglamentarias que se aplican a su industria o al tipo de datos que se están reteniendo. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Los datos de cuentas se conservan únicamente cuando es necesario y por el menor tiempo posible y se eliminan de forma segura o se hacen irrecuperables cuando ya no se necesitan. **Notas de Aplicabilidad** Cuando un TPSP almacena datos de cuentas (por ejemplo, en un entorno de nube), las entidades son responsables de trabajar con sus proveedores de servicios para comprender cómo el TPSP cumple con este requisito para la entidad. Las consideraciones incluyen garantizar que todas las instancias geográficas de un elemento de datos se eliminen de forma segura. *El punto anterior (sobre datos SAD almacenados antes de completar la autorización) es una mejor práctica hasta el 31 de marzo de 2025, después de lo cual se requerirá como parte del Requisito 3.2.1 y se debe considerar en su totalidad durante una evaluación PCI DSS.*		La implementación de un proceso automatizado para garantizar que los datos se eliminen de forma automática y segura dentro de su límite de retención definido, puede ayudar a garantizar que no se retengan más allá de lo necesario para fines de negocios, legales o reglamentarios. Los métodos para eliminar datos cuando excedan el período de retención incluyen la eliminación segura para completar la eliminación de los datos o hacerlos irrecuperables y que no puedan ser reconstruidos. Identificar y eliminar de forma segura los datos almacenados que han excedido su período de retención especificado impide la retención innecesaria de datos que ya no son necesarios. Este proceso puede ser automático, manual o una combinación de ambos. La función de eliminación en la mayoría de los sistemas operativos no es una "eliminación segura" ya que permite recuperar los datos eliminados, por lo que, en su lugar, se debe utilizar una función de eliminación especializada o una aplicación para que los datos sean irrecuperables. *Recuerde, si no lo necesita, ¡no lo guarde!* **Ejemplos** Se podría ejecutar un procedimiento programático automatizado para ubicar y eliminar datos, o se podría realizar una revisión manual de las áreas de almacenamiento de datos. Cualquiera que sea el método utilizado, es buena idea monitorear el proceso para garantizar que se complete exitosamente y que los resultados se registren y validen como completados. La implementación de métodos de eliminación segura garantiza que los datos no se puedan ser recuperados cuando ya no se necesiten. **Información adicional** Consulte el documento NIST SP 800-88 Rev. 1, *Pautas para el Saneamiento de Medios.*

Requisitos y Procedimientos de Prueba		Guía
3.3 Los datos confidenciales de autenticación (SAD) no se almacenan después de la autorización.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
3.3.1 Los SAD no se retienen después de la autorización, incluso si están cifrados. Todos los datos confidenciales de autenticación recibidos se vuelven irrecuperables una vez finalizado el proceso de autorización.	**3.3.1.a** Si se reciben datos SAD, examine las políticas, los procedimientos y las configuraciones del sistema documentados para verificar que no se conserven después de la autorización.	Los SAD son muy útiles para las personas malintencionadas, ya que les permite generar tarjetas de pago falsificadas y realizar transacciones fraudulentas. Por lo tanto, se prohíbe el almacenamiento de los SAD una vez finalizado el proceso de autorización.
	3.3.1.b Si se reciben datos SAD, examine los procedimientos documentados y observe los procesos de eliminación segura de datos para verificar que los datos se vuelvan irrecuperables una vez finalizado el proceso de autorización.	**Definiciones** El proceso de autorización se completa cuando un comerciante recibe una respuesta de transacción (por ejemplo, una aprobación o un rechazo).
Objetivo del Enfoque Personalizado		
Este requisito no es apto para el enfoque personalizado.		
Notas de Aplicabilidad		
Este requisito no se aplica a los emisores y empresas que respaldan los servicios de emisión (en los que los SAD son requeridos para una necesidad legítima de negocio de emisión) y tienen una justificación de negocio para almacenar los datos confidenciales de autenticación. Consulte el Requisito 3.3.3 para conocer los requisitos adicionales específicos para emisores. Los datos confidenciales de autenticación incluyen los datos citados en los Requisitos 3.3.1.1 hasta el 3.3.1.3.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **3.3.1.1** El contenido completo de cualquier pista no se conserva una vez finalizado el proceso de autorización. **Objetivo del Enfoque Personalizado** Este requisito no es apto para el enfoque personalizado. **Notas de Aplicabilidad** En el curso normal de los negocios, es posible que sea necesario conservar los siguientes elementos de datos de la pista: • Nombre del titular de la tarjeta. • Número de cuenta principal (PAN). • Fecha de caducidad. • Código de servicio. Para minimizar el riesgo, almacene de forma segura sólo estos elementos de datos según sea necesario para la empresa.	**Procedimientos de Prueba del Enfoque Definido** **3.3.1.1** Evalúe las fuentes de datos para verificar que el contenido completo de cualquier pista no es almacenado una vez finalizado el proceso de autorización.	**Propósito** Si se almacena el contenido completo de cualquier pista (desde de la banda magnética ubicada en la parte posterior de una tarjeta, si la tiene, o los datos equivalentes contenidos en un chip o en otro lugar), los individuos malintencionados que obtengan esos datos pueden usarlos para reproducir tarjetas de pago y completar transacciones fraudulentas. **Definiciones** Los datos de pista completa se denominan alternativamente datos de pista completa, pista, pista 1, pista 2 y datos de la banda magnética. Cada pista contiene una serie de elementos de datos, y este requisito especifica sólo aquellos que pueden retenerse después de la autorización. **Ejemplos** Las fuentes de datos que deben revisarse para garantizar que el contenido completo de cualquier pista no se conserve una vez finalizado el proceso de autorización incluyen, entre otras: • Datos de transacciones entrantes. • Todos los registros (por ejemplo, transacciones, historial, depuración, error). • Archivos de historial. • Archivos de Rastreo. • Esquemas de bases de datos. • Contenidos de bases de datos, depósitos de datos locales y en la nube. • Cualquier archivo de memoria/archivos de volcado existentes.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **3.3.1.2** El código de verificación de la tarjeta no se conserva una vez finalizado el proceso de autorización. **Objetivo del Enfoque Personalizado** Este requisito no es apto para el enfoque personalizado. **Notas de Aplicabilidad** El código de verificación de la tarjeta es el número de tres o cuatro dígitos impresos en el anverso o reverso de una tarjeta de pago, que se utiliza para verificar las transacciones sin tarjeta presente.	**Procedimientos de Prueba del Enfoque Definido** **3.3.1.2** Evalúe las fuentes de datos para verificar que el código de verificación de la tarjeta no esté almacenado al finalizar el proceso de autorización.	**Propósito** Si se roban los datos del código de verificación de la tarjeta, personas malintencionadas pueden ejecutar transacciones fraudulentas en Internet y realizar pedidos por correo o por teléfono (MO/TO). No almacenar estos datos reduce la probabilidad de que se vean comprometidos. **Ejemplos** Si los códigos de verificación de la tarjeta se almacenan en papel en papel antes de completar la autorización, un método para borrar o cubrir los códigos debería impedir que se lean después de completada la autorización. Ejemplos de métodos para hacer que los códigos sean ilegibles incluyen eliminar el código con unas tijeras y aplicar un marcador adecuadamente opaco e indeleble sobre el código. Las fuentes de datos que se deben revisar para garantizar que el código de verificación de la tarjeta no se conserve una vez finalizado el proceso de autorización incluyen, entre otras: • Datos de transacciones entrantes. • Todos los registros (por ejemplo, transacciones, historial, depuración, error). • Archivos de historial. • Archivos de Rastreo. • Esquemas de bases de datos. • Contenidos de bases de datos, depósitos de datos locales y en la nube. • Cualquier archivo de memoria/archivos de volcado existentes.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Los bloques de PIN y el PIN deben ser conocidos únicamente por el propietario de la tarjeta o por la entidad que emitió la tarjeta. Si se roban estos datos, personas malintencionadas pueden ejecutar transacciones fraudulentas en donde se use el PIN (por ejemplo, compras en tiendas y retiros en cajeros automáticos). No almacenar estos datos reduce la probabilidad de que se vean comprometidos. **Ejemplos** Las fuentes de datos que se deben revisar para garantizar que el PIN y los bloques de PIN no se conserven una vez finalizado el proceso de autorización incluyen, entre otros: • Datos de transacciones entrantes. • Todos los registros (por ejemplo, transacciones, historial, depuración, error). • Archivos de historial. • Archivos de Rastreo. • Esquemas de bases de datos. • Contenidos de bases de datos, depósitos de datos locales y en la nube. • Cualquier archivo de memoria/archivos de volcado existentes.
3.3.1.3 El número de identificación personal (PIN) y el bloque de PIN no se conservan una vez finalizado el proceso de autorización.	**3.3.1.3** Evalúe las fuentes de datos para verificar que los PIN y los bloques de PIN no se almacenan una vez finalizado el proceso de autorización.	
Objetivo del Enfoque Personalizado Este requisito no es apto para el enfoque personalizado.		
Notas de Aplicabilidad Los bloques de PIN se cifran durante el curso natural de los procesos de transacción, pero incluso si una entidad cifra el bloque de PIN nuevamente, todavía no se permite que se almacene después de la finalización del proceso de autorización.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
3.3.2 Los SAD que se almacenan electrónicamente antes de completar la autorización se cifran mediante criptografía sólida.	**3.3.2** Evalúe los repositorios de datos, las configuraciones del sistema y/o la documentación del proveedor para verificar que todos los SAD que se almacenan electrónicamente antes de completar la autorización estén cifrados mediante criptografía sólida.	Los SAD pueden ser utilizados por personas malintencionadas para aumentar la probabilidad de generar transacciones fraudulentas con éxito utilizando tarjetas de pago falsificadas. **Buenas prácticas** Las entidades deben considerar cifrar los SAD con una clave criptográfica diferente a la que se usa para cifrar los datos PAN. Tenga en cuenta que esto no significa que los datos PAN presentes en los SAD (como parte de los datos de pista) deban cifrarse por separado. **Definiciones** El proceso de autorización se completa tan pronto como se recibe la respuesta a una solicitud de autorización, es decir, una aprobación o un rechazo.
Objetivo del Enfoque Personalizado		
Este requisito no es apto para el enfoque personalizado.		
Notas de Aplicabilidad		
Las organizaciones que administran los programas de cumplimiento (por ejemplo, las marcas de pago y adquirentes) determinan si se permite el almacenamiento de los SAD antes de la autorización. Comuníquese con las organizaciones de interés para cualquier criterio adicional. Este requisito aplica para todo almacenamiento de los SAD, incluso si no hay datos PAN en el entorno. Consulte el Requisito 3.2.1 para conocer el requisito adicional que aplica si el SAD se almacena antes de completar la autorización. Este requisito no aplica para los emisores y empresas que respaldan soportan servicios de emisión cuando existe una justificación de negocio legítima de emisión para almacenar los SAD). Consulte el Requisito 3.3.3 para conocer los requisitos específicos para emisores. Este requisito no reemplaza la forma en que se deben administrar los bloques de PIN, ni significa que un bloque de PIN que haya sido cifrado correctamente deba volver a cifrarse. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Los SAD pueden ser utilizados por personas malintencionadas para aumentar la probabilidad de generar con éxito tarjetas de pago falsificadas y realizar transacciones fraudulentas**.** **Buenas prácticas** Las entidades deben considerar cifrar los SAD con una clave criptográfica diferente a la que se usa para cifrar los datos PAN. Tenga en cuenta que esto no significa que los datos PAN presentes en los SAD (como parte de los datos de pista) deban cifrarse por separado. **Definiciones** Necesidad legítima de negocio de emisión significa que los datos son necesarios para facilitar el proceso comercial de emisión. **Información adicional** Refiérase al *ISO/DIS 9564-5 Servicios Financieros - Gestión y Seguridad del Número de Identificación Personal (PIN) - Parte 5: Métodos para la generación, cambio y verificación de los PIN y datos de seguridad de la tarjeta utilizando el estándar de cifrado avanzado.*
3.3.3 ***Requisito adicional para emisores y empresas que soportan servicios de emisión y que almacenan datos confidenciales de autenticación:*** Cualquier almacenamiento de datos confidenciales de autenticación está: • Limitado a lo que se necesita para una necesidad legítima de negocio de emisión y está asegurado. • Cifrado utilizando criptografía. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; refiérase a las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.*	**3.3.3.a** ***Procedimientos de prueba adicionales para emisores y empresas que respaldan servicios de emisión y que almacenan datos confidenciales de autenticación:*** Evalúe las políticas documentadas y entreviste al personal para verificar que existe una justificación de negocio documentada para el almacenamiento de datos confidenciales de autenticación.	
Objetivo del Enfoque Personalizado	**3.3.3.b** ***Pruebas adicionales para emisores y empresas que respaldan*** servicios de emisión ***y que almacenan datos confidenciales de autenticación:*** Evalúe el almacenamiento de datos y las configuraciones del sistema para verificar que los datos confidenciales de autenticación se almacenan de forma segura.	
Los datos confidenciales de autenticación se retienen solo si se requieren respaldar las funciones de emisión y están protegidos contra el acceso no autorizado.		

(continúa en la página siguiente)

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito aplica sólo para los emisores y empresas que respaldan servicios de emisión y almacenan datos confidenciales de autenticación. Las entidades que emiten tarjetas de pago o que realizan o respaldan soportan servicios de emisión a menudo crearán y controlarán datos confidenciales de autenticación como parte de la función de emisión. Está permitido a las empresas que realizan, facilitan o brindan soporte de servicios de emisión, almacenar datos confidenciales de autenticación SÓLO SI se tiene una necesidad legítima de negocio de almacenar dichos datos. Los requisitos de PCI DSS están destinados a todas las entidades que almacenan, procesan o transmiten datos de cuentas, incluidos los emisores. La única excepción para los emisores y procesadores de emisores es que los datos confidenciales de autenticación pueden retenerse si existe una razón legítima para hacerlo. Estos datos deben almacenarse de forma segura y de acuerdo con todas PCI DSS y los requisitos específicos de la marca de pago. *El punto anterior (para cifrar los SAD almacenados con criptografía sólida) es una mejor práctica hasta el 31 de marzo de 2025, después de lo cual se requerirá como parte del Requisito 3.3.3 y se debe considerar por completo durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
3.4 El acceso a las pantallas de datos PAN completas y la capacidad de copiar los datos PAN está restringidos.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** La visualización de datos del PAN completos en las pantallas de ordenadores, los recibos de las tarjetas de pago, los informes en papel, etc., puede dar lugar a que estos datos sean obtenidos por personas no autorizadas y utilizados de forma fraudulenta. Garantizar que la información completa de los datos del PAN se muestre sólo para aquellos con una necesidad legítima de negocios, minimiza el riesgo de que personas no autorizadas accedan a los datos del PAN. **Buenas prácticas** La aplicación de controles de acceso según los roles definidos es una forma de limitar el acceso a la visualización de los datos PAN completos sólo para aquellas personas con una necesidad empresarial definida. El enfoque de enmascaramiento debe mostrar siempre sólo el número de dígitos necesarios para realizar una función empresarial específica. Por ejemplo, si sólo se necesitan los últimos cuatro dígitos para realizar una función empresarial, los datos PAN deben enmascararse para mostrar sólo los últimos cuatro dígitos. Como ejemplo adicional, si una función necesita ver el número de identificación bancaria (BIN) para fines de enrutamiento, desenmascare sólo los dígitos del BIN para esa función. *(continúa en la página siguiente)*
3.4.1 Los datos PAN están enmascarados cuando se muestra (el BIN y los últimos cuatro dígitos **constituyen el número máximo** de dígitos que se muestran), de manera que sólo el personal con una necesidad legítima de negocios pueda ver **más que** el BIN y los últimos cuatro dígitos de los datos PAN. **Objetivo del Enfoque Personalizado** La visualización de datos PAN está restringida al número mínimo de dígitos necesarios para satisfacer una necesidad de negocio definida.	**3.4.1.a** Evalúe las políticas y procedimientos documentados para enmascarar la visualización de los datos PAN a fin de verificar: • Se documenta una lista de funciones que necesitan acceso a más que el BIN y los últimos cuatro dígitos de los datos PAN (incluye el PAN completo), junto con una necesidad legítima de negocios legítima para que cada función tenga dicho acceso. • Los datos PAN se enmascaran cuando se muestran, de modo que sólo el personal con una necesidad legítima de negocios puede ver más que el BIN y los cuatro últimos dígitos de los datos PAN. • Todas las funciones que no estén específicamente autorizadas a ver los datos PAN completos, sólo deben ver los datos PAN enmascarados.	
Notas de Aplicabilidad Este requisito no sustituye a otros más estrictos para la visualización de los datos del titular de la tarjeta, por ejemplo, los requisitos legales o de las marcas de pago para los recibos de los puntos de venta (POS). Este requisito se refiere a la protección de los datos PAN cuando se muestran en pantallas, recibos de papel, impresiones, etc., y no debe confundirse con el requisito 3.5.1 para la protección de los datos PAN cuando se almacenan, procesan o transmiten.	**3.4.1.b** Evalúe las configuraciones del sistema para verificar que los datos del PAN completos sólo se muestran para los roles con una necesidad legítima de negocios, y que los datos del PAN está están enmascarados para todas las demás solicitudes.	

Requisitos y Procedimientos de Prueba		Guía
	3.4.1.c Evalúe la presentación de los datos PAN (por ejemplo, en la pantalla, en los recibos en papel) para verificar que estén enmascarados cuando se muestren, y que sólo aquellos con una necesidad legítima de negocio puedan ver más que el BIN y/o los últimos cuatro dígitos de los datos PAN.	**Definiciones** El enmascaramiento no es sinónimo de truncamiento y estos términos no deben utilizarse indistintamente. El enmascaramiento se refiere a la ocultación de ciertos dígitos durante la visualización o la impresión, incluso cuando los datos PAN completos están almacenados en un sistema. Esto difiere del truncamiento, en el que los dígitos truncados se eliminan y no pueden recuperarse dentro del sistema. Los datos PAN enmascarados pueden ser "desenmascarados", pero no hay "des-truncamiento" sin recrear los datos PAN desde otra fuente. **Información adicional** Para obtener más información sobre el enmascaramiento y el truncamiento, consulte las preguntas frecuentes PCI SCC sobre estos temas.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
3.4.2 Cuando se utilicen tecnologías de acceso remoto, los controles técnicos impiden la copia y/o la reubicación de los datos PAN para todo el personal, excepto para aquellos con autorización explícita y documentada y una necesidad legítima de negocio y definida.	**3.4.2.a** Evalúe las políticas y los procedimientos documentados y las pruebas documentadas de los controles técnicos que impiden la copia y/o la reubicación de los datos PAN cuando se utilizan tecnologías de acceso remoto en discos duros locales o medios electrónicos extraíbles para verificar lo siguiente: • Los controles técnicos impiden que todo el personal no autorizado específicamente copie y/o reubique los datos PAN. • Se mantiene una lista del personal con permiso para copiar y/o reubicar los datos PAN, junto con la autorización explícita y documentada y la necesidad legítima de negocio y definida.	La reubicación de los datos PAN a dispositivos de almacenamiento no autorizados es una forma común de obtener y utilizar esta información de manera fraudulenta. Los métodos para garantizar que sólo aquellos con autorización explícita y una razón comercial legítima puedan copiar o reubicar los datos PAN minimizan el riesgo de que personas no autorizadas obtengan acceso a los datos PAN.
Objetivo del Enfoque Personalizado		**Buenas prácticas**
Los datos PAN no pueden ser copiados ni reubicados por personal no autorizado que utilice tecnologías de acceso remoto.		La copia y reubicación de los datos PAN sólo debe hacerse en dispositivos de almacenamiento permitidos y autorizados para esa persona.
Notas de Aplicabilidad	**3.4.2.b** Evalúe las configuraciones de las tecnologías de acceso remoto para confirmar que los controles técnicos impiden la copia y/o reubicación de los PAN para todo el personal, a menos que se autorice explícitamente.	**Definiciones** El escritorio virtual es un ejemplo de tecnología de acceso remoto. Los dispositivos de almacenamiento incluyen, entre otros, discos duros locales, unidades virtuales, medios electrónicos extraíbles, unidades de red y almacenamiento en la nube.
Almacenar o reubicar los datos PAN en discos duros locales, medios electrónicos extraíbles y otros dispositivos de almacenamiento hace que estos dispositivos estén dentro del alcance PCI DSS. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**3.4.2.c** Observe los procesos y entreviste al personal para verificar que solo el personal con autorización explícita documentada y una necesidad legítima de negocio y definida tenga permiso para copiar y/o reubicar los datos PAN cuando utilice tecnologías de acceso remoto.	**Información adicional** La documentación del proveedor de la tecnología de acceso remoto en uso proporcionará información sobre la configuración del sistema necesaria para aplicar este requisito.

Requisitos y Procedimientos de Prueba		Guía
3.5 El número de cuenta principal (PAN) está protegido donde sea que se almacene.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
3.5.1 Los datos PAN se hacen ilegibles en cualquier lugar donde se almacenen utilizando cualquiera de los siguientes enfoques: • *Hashes* unidireccionales basados en criptografía sólida del PAN completo. • Truncamiento (los *hashes* no pueden utilizarse para reemplazar el segmento truncado de la PAN). – Si en un entorno hay versiones truncadas y con *hash* del mismo PAN, o diferentes formatos de truncamiento del mismo PAN, se establecen controles adicionales de manera que las diferentes versiones no puedan correlacionarse para reconstruir el PAN original. • Índice de tokens. • Criptografía robusta con procesos y procedimientos de gestión de claves asociados.	**3.5.1.a** Evalúe la documentación del sistema utilizado para hacer ilegibles los datos del PAN, incluido el proveedor, el tipo de sistema/proceso y los algoritmos de cifrado (si procede) para verificar que los datos del PAN se hacen ilegibles utilizando cualquiera de los métodos especificados en este requisito. **3.5.1.b** Evalúe el almacenamiento de los datos y los registros de auditoría para verificar que los PAN se hace ilegibles utilizando cualquiera de los métodos especificados en este requisito. **3.5.1.c** Si hay versiones truncadas y con *hash* de los mismos datos PAN en el entorno, examine los controles implementados para verificar que las versiones truncadas y con *hash* no pueden correlacionarse para reconstruir los datos PAN originales.	**Propósito** La eliminación de los datos PAN almacenados en texto en claro constituye un sólido control de defensa a fondo diseñado para proteger los datos almacenados por si una persona no autorizada obtiene acceso a ellos aprovechando una vulnerabilidad o una configuración incorrecta del control de acceso primario de una entidad. Los sistemas de control secundarios independientes (por ejemplo, que rigen el acceso y el uso de claves de cifrado y descifrado) impiden la falla de un sistema de control de acceso primario que conduce a una violación de la confidencialidad de los datos PAN almacenados. Si se utiliza *hash* para eliminar los datos PAN de texto sin cifrar almacenados, al correlacionar versiones de *hash* y truncadas de datos PAN determinados, individuos malintencionados pueden derivar fácilmente el valor de los datos PAN originales. Los controles para impedir la correlación de estos datos ayudarán a garantizar que el PAN original permanezca ilegible. **Información adicional** Para obtener información sobre los formatos de truncamiento y el truncamiento en general, consulte las preguntas frecuentes PCI SCC sobre el tema. Las fuentes de información del índice de tokens incluyen: • Directrices de Seguridad de Productos con Token PCI SCC *(https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf)* *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Los datos del PAN en texto claro no pueden ser leídos desde los medios de almacenamiento.		• *ANSI X9.119-2-2017: Servicios Financieros Al por Menor - Requisitos para la Protección de los Datos Confidenciales de las Tarjetas de Pago - Parte 2: Implementación de Sistemas de Tokenización Post-Autorización*
Notas de Aplicabilidad Constituye un esfuerzo relativamente trivial para individuos malintencionados el reconstruir los datos del PAN originales si tienen acceso tanto a la versión truncada como a la versión *hash* de una PAN. Este requisito se aplica a los datos PAN guardados en almacenamiento primario (bases de datos o archivos planos como hojas de cálculo de archivos de texto), así como en almacenamiento no primario (copias de seguridad, registros de auditoría, registros de excepciones o de resolución de problemas), todos ellos deben estar protegidos. Este requisito no excluye el uso de archivos temporales que contengan datos PAN en texto no cifrado mientras se encriptan y des-encriptan.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
3.5.1.1 Los *hash* utilizados para hacer ilegibles los datos PAN (según el primer punto del requisito 3.5.1) son *hashes* criptográficos con clave de todos los datos PAN, con procesos y procedimientos de gestión de claves asociados de acuerdo con los Requisitos 3.6 y 3.7.	**3.5.1.1.a** Evalúe la documentación referente al método de *hashing* utilizado para hacer ilegibles los datos PAN, incluyendo el proveedor, el tipo de sistema/proceso y los algoritmos de cifrados (según proceda) para verificar que el método de *hashing* da como resultado *hashes* criptográficos con clave de todos los datos PAN, con los procesos y procedimientos de gestión de claves asociados.	**Objetivo** La eliminación del PAN almacenado en texto no cifrado constituye un sólido control de defensa diseñado para proteger los datos si una persona no autorizada obtiene acceso a los datos almacenados aprovechando una vulnerabilidad o una configuración errónea del control de acceso principal de una entidad. Los sistemas de control secundarios independientes (por ejemplo, los que rigen el acceso y el uso de las claves de criptografía y descifrado) impiden que el fallo de un sistema de control de acceso primario provoque una violación de la confidencialidad de los datos PAN almacenados. **Buenas Prácticas** Una función de *hash* que incorpore una clave secreta generada aleatoriamente proporciona resistencia a los ataques de fuerza bruta e integridad del secreto autenticación. **Información Adicional** Los algoritmos *hashing* criptográficos en clave adecuados incluyen, entre otros, los siguientes: HMAC, CMAC y GMAC, con fuerza criptográfica efectiva de al menos 128 bits *(NIST SP 800-131Ar2).* Refiérase a los siguientes para obtener más información sobre HMAC, CMAC y GMAC, respectivamente: *NIST SP 800-107r1, NIST SP 800-38B y NIST SP 800-38D).* *Véase NIST SP 800-107 (Revisión 1): Recomendación para Aplicaciones que Utilizan Algoritmos Hash Aprobados §5.3.*
Notas de Aplicabilidad	**3.5.1.1.b** Evalúe los documentos de los procedimientos de gestión de claves y procesos asociados con los *hashes* criptográficos con clave, para verificar que las claves se gestionan de acuerdo con los Requisitos 3.6 y 3.7.	
Este requisito se aplica a los datos PAN guardados en almacenamiento primario (bases de datos o archivos planos como hojas de cálculo de archivos de texto), así como en almacenamiento no primario (copias de seguridad, registros de auditoría, registros de excepciones o de resolución de problemas), todos ellos deben estar protegidos. Este requisito no excluye el uso de archivos temporales que contengan datos PAN en texto no cifrado mientras se encriptan y des-encriptan. *Este requisito se considera una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**3.5.1.1.c** Evalúe los repositorios de datos para verificar que los datos PAN aparezcan ilegibles.	
	3.5.1.1.d Evalúe los registros de auditoría, incluidos los registros de la aplicación de pagos, para verificar que los datos PAN se han vuelto ilegibles.	

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
3.5.1.2 Si se utiliza un cifrado a nivel de disco o de partición (en lugar de un cifrado de base de datos a nivel de archivo, columna o campo) para hacer que los datos PAN sea ilegibles, sólo se implementará de la siguiente manera: • En medios electrónicos extraíbles, **O** • Si se utiliza para medios electrónicos no extraíbles, los datos PAN también se hacen ilegibles mediante otro mecanismo que cumpla con el Requisito 3.5.1.	**3.5.1.2.a** Evalúe los procesos de cifrado para verificar que, si se utiliza el cifrado a nivel de disco o de partición para hacer ilegibles los datos PAN, que éste sea implementado sólo como sigue: • En medios electrónicos extraíbles, **O** • Si se utilizan para medios electrónicos no extraíbles, examine los procesos de cifrado utilizados para verificar que los datos PAN también se hacen ilegibles mediante otro método que cumpla el requisito 3.5.1.	**Objetivo** El cifrado a nivel de disco y de partición suele cifrar todo el disco o la partición utilizando la misma clave con todos los datos descifrados automáticamente cuando el sistema se ejecuta o cuando un usuario autorizado lo solicita. Por esta razón, el cifrado a nivel de disco no es apropiado para proteger los datos PAN almacenados en ordenadores, portátiles, servidores, matrices de almacenamiento o cualquier otro sistema que proporcione un descifrado transparente tras la autenticación del usuario. **Información Adicional** En caso de estar disponibles, seguir las directrices de *hardening* y mejores prácticas del sector para los proveedores, pueden ayudar a proteger los datos PAN en estos dispositivos.
Objetivo del Enfoque Personalizado	**3.5.1.2.b** Evalúe las configuraciones y/o los documentos del proveedor y observe los procesos de cifrado para verificar que el sistema está configurado de acuerdo con los documentos del proveedor y que el resultado es que el disco o la partición se vuelven ilegibles.	
Este requisito no es apto para el enfoque personalizado. *(continúa en la página siguiente)*		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad		
Aunque el cifrado de disco puede seguir estando presente en estos tipos de dispositivos, este no puede ser el único mecanismo utilizado para proteger los datos del PAN almacenados en esos sistemas. Cualquier dato del PAN almacenado también debe volverse ilegible según el Requisito 3.5.1, por ejemplo, mediante el truncamiento o por un mecanismo de cifrado a nivel de datos. El cifrado de disco completo ayuda a proteger los datos en caso de pérdida física de un disco y, por lo tanto, su uso es apropiado sólo para dispositivos de almacenamiento de medios electrónicos extraíbles. Los medios que forman parte de la arquitectura de un centro de datos (por ejemplo, unidades intercambiables en caliente, copias de seguridad en cinta) se consideran medios electrónicos no extraíbles a los que se aplica el Requisito 3.5.1. Las implementaciones de cifrado de discos o particiones también deben cumplir todos los demás requisitos de cifrado y gestión de claves PCI DSS. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
3.5.1.3 Si se utiliza el cifrado a nivel del disco o de partición (en lugar del cifrado de la base de datos a nivel de archivo, columna o campo) para hacer que los datos PAN sea ilegibles, sólo se implementará de la siguiente manera: • El acceso lógico se gestiona por separado e independientemente de la autenticación del sistema operativo nativo y de los mecanismos de control de acceso. • Las claves de descifrado no están asociadas a las cuentas de usuario.	**3.5.1.3.a** Si se utiliza el cifrado a nivel de disco o de partición para hacer ilegibles los datos PAN, examine la configuración del sistema y observe el proceso de autenticación para verificar que el acceso lógico se implementa de acuerdo con todos los elementos especificados en este requisito.	El cifrado a nivel de disco suele cifrar todo el disco o la partición utilizando la misma clave, y todos los datos se descifran automáticamente cuando el sistema se ejecuta o cuando un usuario autorizado lo solicita. Muchas soluciones de encriptación de disco interceptan las operaciones de lectura/escritura del sistema operativo y realizan las transformaciones criptográficas apropiadas sin necesidad de ninguna acción especial por parte del usuario, aparte de proporcionar una contraseña o frase de paso al iniciar el sistema o al comienzo de una sesión. Esto no proporciona ninguna protección frente a individuos malintencionados que ya hayan conseguido ingresar a una cuenta de usuario válida.
Objetivo del Enfoque Personalizado	**3.5.1.3.b** Examine los archivos y entreviste al personal para verificar que las contraseñas, las frases de contraseña o las claves criptográficas que permiten el acceso a los datos no cifrados se almacenan de forma segura y son independientes de los métodos de autenticación y control de acceso del sistema operativo nativo.	**Buenas Prácticas**
Las implementaciones de cifrado de disco están configuradas para requerir autenticación independiente y controles de acceso lógico para el descifrado.		El cifrado de todo el disco ayuda a proteger los datos en caso de pérdida física de un disco y, por lo tanto, es mejor limitar su uso solamente a los dispositivos de almacenamiento de medios electrónicos extraíbles.
Notas de Aplicabilidad		
Las implementaciones de cifrado de discos o particiones también deben cumplir todos los demás requisitos de cifrado y gestión de claves PCI DSS.		

Requisitos y Procedimientos de Prueba		Guía
3.6 Las claves criptográficas utilizadas para proteger los datos de cuentas almacenadas están protegidas.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
3.6.1 Los procedimientos se definen e implementan para proteger las claves cifradas utilizadas para proteger los datos almacenados de la cuenta contra la divulgación y el uso indebido que incluyen: • El acceso a las claves está restringido al menor número de custodios necesarios. • Las claves de cifrado de claves son al menos tan seguras como las claves de cifrado de datos que estas protegen. • Las claves de cifrado de claves se almacenan por separado de las claves de cifrado de datos. • Las claves se almacenan de forma segura en el menor número posible de formas y ubicaciones.	**3.6.1** Evalúe las políticas y los procedimientos documentados de administración de claves para verificar que los procesos para proteger las claves cifradas utilizadas para proteger los datos almacenados de la cuenta contra la divulgación y el uso indebido estén definidos para incluir todos los elementos especificados en este requisito.	Las claves criptográficas deben estar fuertemente protegidas porque debido a que aquellos que obtengan tengan acceso a ellas podrán descifrar los datos. **Buenas Prácticas** Se recomienda tener un sistema de administración de claves centralizado basado en los estándares de la industria para administrar las claves cifradas. **Información Adicional** Los procedimientos de gestión de claves de la entidad se beneficiarán a través de la alineación con los requisitos de la industria. Las fuentes de información sobre los ciclos de vida de la gestión de claves cifradas incluyen: • *ISO 11568-1 Banca - Gestión de claves (minoristas) - Parte 1*: Principios (específicamente el Capítulo 10 y las Partes 2 y 4 a las que se hace referencia) • *NIST SP 800-57 Parte 1 Revisión 5 — Recomendación para la Administración de Claves, Parte 1: General*.
Objetivo del Enfoque Personalizado		
Se definen e implementan procesos que protegen las claves criptográficas utilizadas para proteger los datos de cuentas almacenados contra la divulgación y el uso indebido.		
(continúa en la página siguiente)		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito se aplica a las claves utilizadas para cifrar los datos de cuentas almacenados y a las claves de cifrado utilizadas para proteger las claves de cifrado de datos. El requisito de proteger las claves utilizadas para proteger los datos almacenados de la cuenta de la divulgación y el uso indebido se aplica tanto a las claves de cifrado de datos como a las claves de cifrado de claves. Debido a que una clave de cifrado de claves puede otorgar acceso a muchas claves de cifrado de datos, las claves de cifrado de claves requieren fuertes medidas de protección.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Mantener la documentación de la arquitectura criptográfica actualizada le permite a la entidad comprender los algoritmos, protocolos y claves criptográficas que se utilizan para proteger los datos de cuentas almacenados, así como los dispositivos que generan, usan y protegen las claves. Esto le permite a la entidad mantenerse al día con las amenazas en progreso contra su arquitectura y planificar actualizaciones a medida que cambia el nivel de protección proporcionado por los cambios en los algoritmos y la fortaleza de las claves. El mantenimiento de dicha documentación también permite que la entidad detecte claves perdidas o faltantes o los dispositivos de administración de claves e identificar adiciones no autorizadas a su arquitectura criptográfica. El uso de las mismas claves criptográficas en los entornos de producción y de prueba presenta el riesgo de exponer la clave si el entorno de prueba no tiene el mismo nivel de seguridad que el entorno de producción.
3.6.1.1 ***Requisito adicional sólo para proveedores de servicios:*** Se mantiene una descripción documentada de la arquitectura criptográfica que incluye: • Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos de la cuenta almacenados, incluyendo la fuerza de la clave y la fecha de caducidad. • Evitar el uso de las mismas claves criptográficas en entornos de producción y de prueba. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; consulte las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.* • Descripción del uso de claves para cada clave. • Inventario de los módulos de seguridad de hardware (HSM), sistemas de gestión de claves (KMS) y otros dispositivos criptográficos seguros (SCD) utilizados para la gestión de claves, incluido el tipo y la ubicación de los dispositivos, como se describe en el Requisito 12.3.4.	**3.6.1.1** ***Procedimiento de prueba adicional sólo para evaluaciones de proveedores de servicios:*** Entreviste al personal responsable y examine la documentación para verificar que existe un documento que describa la arquitectura criptográfica y que incluya todos los elementos especificados en este requisito.	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Los detalles precisos de la arquitectura criptográfica se mantienen y están disponibles.		**Buenas Prácticas** Tener un mecanismo de informes automatizado puede ayudar con el mantenimiento de los atributos criptográficos.
Notas de Aplicabilidad Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios. En las implementaciones de HSM en la nube, la responsabilidad de la arquitectura criptográfica de acuerdo con este Requisito será compartida entre el proveedor de la nube y el cliente de la nube. *El punto anterior (para que en la arquitectura criptográfica se impida el uso de las mismas claves criptográficas en producción y prueba) es una mejor práctica hasta el 31 de marzo de 2025, después de lo cual se requerirá como parte del Requisito 3.6.1.1 y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
3.6.1.2 Las claves secretas y privadas que se utilizan para cifrar/descifrar los datos de la cuenta se almacenan en una (o más) de las siguientes formas en todo momento: • Cifrado con una clave de cifrado de clave, que sea al menos tan fuerte, como la clave de cifrado de datos y que se almacene por separado de la clave de cifrado de datos. • Dentro de un dispositivo criptográfico seguro (SCD), como un módulo de seguridad de hardware (HSM) o un dispositivo de punto de interacción aprobado por PTS. • Como, al menos, dos componentes de clave de longitud completa o claves compartidas de acuerdo con un método aceptado por la industria.	**3.6.1.2.a** Evalúe los procedimientos documentados para verificar que se define que las claves criptográficas utilizadas para cifrar/descifrar los datos de cuentas almacenados deben existir sólo en una (o más) de las formas especificadas en este requisito. **3.6.1.2.b** Evalúe las configuraciones del sistema y las ubicaciones de almacenamiento de claves para verificar que las claves criptográficas utilizadas para cifrar/descifrar los datos del tarjetahabiente almacenados existan en una (o más) de las formas especificadas en este requisito. **3.6.1.2.c** Dondequiera que se utilicen claves de cifrado de claves, examine las configuraciones del sistema y las ubicaciones de almacenamiento de claves para verificar: • Las claves de cifrado de claves son al menos tan seguras como las claves de cifrado de datos que estas protegen. • Las claves de cifrado de claves se almacenan por separado de las claves de cifrado de datos.	**Objetivo** El almacenamiento de claves criptográficas de forma segura impide el acceso no autorizado o innecesario que podría resultar de la exposición de los datos almacenados del tarjetahabiente la cuenta. Almacenar claves por separado significa que se almacenan de manera tal, que, si la ubicación de una clave se ve comprometida, la segunda clave permanece segura. No lo estará también **Buenas Prácticas** Cuando las claves de cifrado de datos se almacenan en un HSM, el canal de interacción del HSM debería protegerse para impedir la interceptación de las operaciones de cifrado o descifrado.
Objetivo del Enfoque Personalizado		
Las claves secretas y privadas se almacenan de forma segura impidiendo la recuperación o el acceso no autorizados.		

(continúa en la página siguiente)

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad No es necesario que las claves públicas sean almacenadas en una de estas formas. Las claves criptográficas almacenadas como parte de un sistema de gestión de claves (KMS) que emplea SCD son aceptables. Una clave criptográfica que se divide en dos partes no cumple con este requisito. Las claves secretas o privadas almacenadas como componentes clave o recursos compartidos de claves deben generarse a través de uno de los siguientes: • Utilizando un generador de números aleatorios aprobado y dentro de un SCD, **O** • De acuerdo con el Estándar ISO 19592 o su equivalente en la industria para la generación de claves secretas compartidas.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **3.6.1.3** El acceso a los componentes de claves criptográficas de texto no cifrado está restringido al menor número posible de custodios que sean necesarios. **Objetivo del Enfoque Personalizado** El acceso a los componentes de claves criptográficas de texto no cifrado está restringido al personal necesario.	**Procedimientos de Prueba del Enfoque Definido** **3.6.1.3** Evalúe las listas de acceso de los usuarios para verificar que el acceso a los componentes de claves criptográficas de texto no cifrado esté restringido al menor número posible de custodios que sean necesarios.	**Objetivo** Restringir el número de personas que tienen acceso a componentes de claves criptográficas de texto no cifrado reduce el riesgo de que los datos de la cuenta almacenados sean recuperados o visibilizados por individuos no autorizados. **Buenas Prácticas** Solo el personal con responsabilidades definidas de custodia de claves (creación, alteración, rotación, distribución o mantenimiento de claves de cifrado) debe tener acceso a los componentes clave. Idealmente, será un número muy reducido de personas.
Requisitos del Enfoque Definido **3.6.1.4** Las claves criptográficas se almacenan en el menor número posible de ubicaciones. **Objetivo del Enfoque Personalizado** Las claves criptográficas se conservan sólo cuando es necesario.	**Procedimientos de Prueba del Enfoque Definido** **3.6.1.4** Evalúe las ubicaciones de almacenamiento de claves y observe los procesos para verificar que las claves son almacenadas en la menor cantidad posible de ubicaciones.	**Objetivo** El almacenamiento de las claves criptográficas en la menor cantidad posible de ubicaciones contribuye a que la organización pueda rastrear y monitorear todas las ubicaciones de las claves y minimiza la posibilidad de que las claves estén expuestas a partes no autorizadas.

Requisitos y Procedimientos de Prueba		Guía
3.7 Cuando se usa criptografía para proteger datos de cuentas almacenados, se definen e implementan procesos y procedimientos de administración de claves que cubren todos los aspectos del ciclo de vida de las claves.		
Requisitos del Enfoque Definido **3.7.1** Las políticas y procedimientos de administración de claves se implementan para incluir la generación de claves criptográficas fuertes utilizadas para proteger los datos de cuentas almacenados. **Objetivo del Enfoque Personalizado** Generación de claves criptográficas fuertes.	**Procedimientos de Prueba del Enfoque Definido** **3.7.1.a** Evalúe las políticas y procedimientos documentados de gestión de claves utilizados para la protección de los datos de cuentas almacenados a fin de verificar que definan la generación de claves criptográficas fuertes. **3.7.1.b** Observe el método para generar claves para verificar que se generen claves fuertes.	**Objetivo** El uso de claves criptográficas sólidas aumenta significativamente el nivel de seguridad de los datos de cuentas cifrados. **Información Adicional** Consulte las fuentes a las que se hace referencia en "Generación de Claves Criptográficas en Anexo G".
Requisitos del Enfoque Definido **3.7.2** Las políticas y los procedimientos de administración de claves son implementados para incluir la distribución segura de las claves criptográficas utilizadas para proteger los datos almacenados de la cuenta. **Objetivo del Enfoque Personalizado** Las claves criptográficas están protegidas durante la distribución.	**Procedimientos de Prueba del Enfoque Definido** **3.7.2.a** Evalúe las políticas y procedimientos documentados de administración de claves para las claves de protección de los datos de cuentas almacenados a fin de verificar que definen la distribución segura de claves criptográficas. **3.7.2.b** Observe el método para distribuir claves a fin de verificar que las claves se distribuyan de forma segura.	**Objetivo** La distribución o transmisión segura de claves criptográficas secretas o privadas significa que las claves sólo son distribuidas a los custodios autorizados, como se identifica en el Requisito 3.6.1.2, y nunca se distribuyen de forma insegura.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Almacenar las claves sin la debida protección podría dar acceso a los atacantes, lo que provocaría el descifrado y la exposición de los datos de la cuenta. **Buenas Prácticas** Las claves de cifrado de datos pueden protegerse cifrándolas con una clave de cifrado de clave. Las claves pueden almacenarse en un Módulo de Seguridad de Hardware (HSM). Las claves secretas o privadas que pueden descifrar datos nunca deben estar presentes en el código fuente.
3.7.3 Se implementan políticas y procedimientos de gestión de claves para incluir el almacenamiento seguro de las claves criptográficas utilizadas para proteger los datos de cuentas almacenados.	**3.7.3.a** Evalúe las políticas y procedimientos documentados de administración de claves utilizados para las claves de protección de los datos de cuentas almacenados a fin de verificar que definen el almacenamiento seguro de claves criptográficas.	
	3.7.3.b Observe el método de almacenamiento de claves para verificar que las claves se almacenan de forma segura.	
Objetivo del Enfoque Personalizado		
Las claves criptográficas están protegidas cuando se almacenan.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Es imprescindible cambiar las claves de cifrado cuando llegan al final de su criptoperíodo a fin de minimizar el riesgo de que alguien obtenga las claves de cifrado y las utilice para descifrar datos. **Definiciones** Un criptoperíodo es el lapso de tiempo durante el cual una clave criptográfica puede ser utilizada para su propósito definido. Los criptoperíodos suelen definirse en términos del periodo durante el cual la clave está activa y/o la cantidad de texto cifrado que ha producido la clave. Las consideraciones para definir el criptoperíodo incluyen, pero no se limitan a, la fuerza del algoritmo subyacente, el tamaño o la longitud de la clave, el riesgo de compromiso de la clave y la sensibilidad de los datos que se cifran. (continúa en la página siguiente)
3.7.4 Se implementan políticas y procedimientos de gestión de claves para los cambios de claves criptográficas de para aquellas claves que han llegado al final de su criptoperíodo, según lo definido por el proveedor de la aplicación asociada o el propietario de la clave, y basado en las mejores prácticas y directrices de la industria, incluyendo lo siguiente: • Un criptoperíodo definido para cada tipo de clave en uso. • Un proceso para el cambio de claves al final del criptoperíodo definido.	**3.7.4.a** Evalúe las políticas y los procedimientos documentados de gestión de claves utilizados para la protección de los datos de cuentas almacenados a fin de verificar que definen los cambios de las claves criptográficas que han llegado al final de su criptoperíodo e incluyen todos los elementos especificados en este requisito.	
	3.7.4.b Entreviste al personal, examine la documentación y observe las ubicaciones de almacenamiento de claves para verificar que las claves se cambian al final de los criptoperíodos definidos.	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Las claves criptográficas no se utilizan más allá de su criptoperíodo definido.		**Información Adicional** *NIST SP 800-57 Parte 1, Revisión 5, Sección 5.3 criptoperíodos - Se brinda orientación para establecer el lapso de tiempo durante el cual una clave específica está autorizada para ser usada por entidades legítimas, o las claves para un determinado sistema permanecerán en vigor.* Refiérase a la Tabla 1 de *SP 800-57* Parte 1 para criptoperíodos sugeridos para diferentes tipos de claves.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
3.7.5 Los procedimientos de políticas de gestión de claves se implementan para incluir el retiro, sustitución o destrucción de las claves utilizadas para proteger los datos de cuentas almacenados, según se considere necesario cuando: • La clave haya llegado al final de su criptoperíodo definido. • La integridad de la clave se haya debilitado, incluso cuando el personal con conocimiento de un componente de la clave en texto no cifrado abandone la empresa, o la función por la que conocía la clave. • Cuando se sospecha o se sabe que las claves están comprometidas. Las claves retiradas o reemplazadas no se utilizan para operaciones de cifrado.	**3.7.5.a** Evalúe las políticas y los procedimientos documentados de gestión de claves utilizados para la protección de los datos de cuentas almacenadas y verifique que definen el retiro, el reemplazo o la destrucción de las claves de acuerdo con todos los elementos especificados en este requisito.	Las claves que ya no son necesarias, las claves con integridad debilitada y las claves que se sabe o se sospecha que están comprometidas, deben ser archivadas, revocadas y/o destruidas para asegurarse de ya no puedan ser utilizadas. Si es necesario conservar dichas claves (por ejemplo, para respaldar los datos cifrados), estas deben estar fuertemente protegidas.
Objetivo del Enfoque Personalizado	**3.7.5.b** Entreviste al personal para verificar que los procesos son implementados de acuerdo con todos los elementos especificados en este requisito.	**Buenas Prácticas** Las claves criptográficas archivadas deberían utilizarse únicamente para fines de descifrado/verificación. La solución de cifrado debe proveer y facilitar un proceso para sustituir las claves que deban ser reemplazadas o que se sepa o se sospeche que están, comprometidas. Además, cualquier clave que se sepa o se sospeche que está comprometida, debe gestionarse de acuerdo con el plan de respuesta a incidentes de la entidad descrito en el Requisito 12.10.1.
Las claves se retiran del uso activo cuando se sospecha o se sabe que la integridad de la clave está debilitada.		**Información Adicional** Las mejores prácticas de la industria para archivar las claves retiradas se describen en el documento *NIST SP 800-57 Parte 1, Revisión 5, Sección 8.3.1*, e incluyen el mantenimiento del archivo con terceros confiables y el almacenamiento de la información de las claves archivadas por separado de los datos operativos.
Notas de Aplicabilidad		
Si es necesario conservar las claves criptográficas retiradas o reemplazas, dichas claves deben archivarse de forma segura (por ejemplo, utilizando una clave de cifrado).		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
3.7.6 Cuando el personal realiza operaciones manuales de gestión de claves criptográficas en texto no cifrado, se implementan políticas y procedimientos de gestión de claves que incluyen la gestión de estas operaciones utilizando conocimiento dividido y control dual.	**3.7.6.a** Evalúe las políticas y procedimientos documentados de administración de claves para las claves utilizadas para la protección de datos de cuentas almacenados y verifique que se definan utilizando conocimiento dividido y control dual. **3.7.6.b** Entreviste al personal y/u observe los procesos para verificar que las claves manuales de texto no cifrado se manejen con conocimiento dividido y control dual.	El conocimiento dividido y el doble control de las claves se utilizan para eliminar la posibilidad de que una sola persona tenga acceso a toda la clave, y por ende pueda obtener accesos no autorizado a los datos. **Definiciones** El conocimiento dividido es un método en el que dos o más personas tienen por separado componentes de la clave, en el que cada persona sólo conoce su propio componente de la clave, y los componentes individuales de la clave no transmiten ningún conocimiento de otros componentes o de la clave criptográfica original. El control dual requiere que dos o más personas autentiquen el uso de una clave criptográfica o realicen una función de gestión de claves. Ninguna persona puede acceder o utilizar el factor de autenticación (por ejemplo, la contraseña, el PIN o la clave) de otra. **Buenas Prácticas** Cuando se utilicen componentes clave o recursos compartidos de claves, los procedimientos deben garantizar que ningún custodio tenga acceso a suficientes componentes de la clave o recursos compartidos para reconstruir la clave criptográfica. Por ejemplo, en un esquema m-de-n (por ejemplo, Shamir), donde solo se requieren dos de los tres componentes para reconstruir la clave criptográfica, un custodio no debe tener conocimiento actual o previo de más de un componente. Si a un custodio se le asignó previamente el componente A, que luego fue reasignado, no se le debe asignar al custodio el componente B o C, ya que esto le daría al custodio el conocimiento de dos componentes y la capacidad de recrear la clave. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado		
Nadie puede conocer las claves secretas o privadas de texto no cifrado. Las operaciones que involucran claves de texto no cifrado no pueden ser realizadas por una sola persona.		
Notas de Aplicabilidad		
Este control es aplicable para operaciones manuales de administración de claves o donde la administración de claves no está controlada por el producto de cifrado. Una clave criptográfica que simplemente se divide en dos partes no cumple con este requisito. Las claves secretas o privadas almacenadas como componentes clave o recursos compartidos de claves deben generarse a través de uno de los siguientes métodos: • Utilizando un generador de números aleatorios aprobado y dentro de un dispositivo criptográfico seguro (SCD), como un módulo de seguridad de hardware (HSM) o un dispositivo de punto de interacción aprobado por PTS, **O** • De acuerdo con el Estándar ISO 19592 o su equivalente en la industria para la generación de claves secretas compartidas.		

Requisitos y Procedimientos de Prueba		Guía
		Ejemplos Las operaciones de administración de claves que se pueden realizar manualmente incluyen, entre otras, la generación, transmisión, carga, almacenaje y destrucción de claves. **Información Adicional** Los estándares de la industria para la gestión de componentes de claves incluyen: • *NIST SP 800-57* Parte 2 Revisión 1 — Recomendación para la Administración de Claves. Parte 2 - Mejores Prácticas para Organizaciones de Gestión de Claves [4.6 Distribución de Material de Claves] • *ISO 11568-2 Banca - Gestión de claves (minoristas) - Parte 2*: Cifrados simétricos, su gestión de claves y ciclo de vida [4.7.2.3 Componentes de Claves y 4.9.3 Componentes de Claves] • *Consejo Europeo de Pagos EPC342-08 Directrices del Sobre el Uso de Algoritmos Criptográficos y la Gestión de Claves* [especialmente 4.1.4 Instalación de Claves].

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Si un atacante puede sustituir la clave de una entidad con una clave que el atacante conoce, el atacante podrá descifrar todos los datos cifrados con esa clave. **Buenas Prácticas** La solución de cifrado no debe permitir ni aceptar la sustitución de claves de fuentes no autorizadas o procesos inesperados. Los controles deben incluir garantizar que las personas con acceso a componentes o recursos compartidos de claves no tengan acceso a otros componentes o recursos compartidos que formen el umbral necesario para obtener la clave.
3.7.7 Se implementan políticas y procedimientos de administración de claves para incluir la prevención de la sustitución no autorizada de claves criptográficas.	**3.7.7.a** Evalúe las políticas y procedimientos documentados de administración de claves para las claves utilizadas para la protección de datos de cuenta almacenados y verifique que definan la prevención de la sustitución no autorizada de claves criptográficas.	
Objetivo del Enfoque Personalizado		
Las claves criptográficas no pueden ser sustituidas por personal no autorizado.	**3.7.7.b** Entreviste al personal y/u observe los procesos para verificar que se impida la sustitución no autorizada de claves.	
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Este proceso ayudará a garantizar que las personas que actúan como custodios de claves se comprometan con el rol de custodios de claves y comprendan y acepten sus responsabilidades. Una reafirmación anual puede ayudar a recordar a los custodios de claves sus responsabilidades. **Información Adicional** La guía de la industria para los custodios de claves y sus roles y responsabilidades incluye: • *NIST SP 800-130 Un Marco para Diseñar Sistemas de Administración de Claves Criptográficas* [5. Funciones y Responsabilidades (especialmente) para los Custodios de Claves] • *ISO 11568-1 Banca - Gestión de claves (minoristas) --Parte 1*: Principios [5 Principios de la Gestión de Claves (especialmente b)]
3.7.8 Las políticas y los procedimientos de administración de claves se implementan para incluir que los custodios de claves criptográficas reconozcan formalmente (por escrito o electrónicamente) que comprenden y aceptan sus responsabilidades como custodios de claves.	**3.7.8.a** Evalúe las políticas y procedimientos documentados de administración de claves para las claves utilizadas en la protección de datos de cuentas almacenados y verifique que definen el reconocimiento por parte de los custodios de las claves de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado		
Los custodios de claves reconocen sus responsabilidades con relación a las operaciones criptográficas y pueden obtener asistencia y orientación cuando sea necesario.	**3.7.8.b** Evalúe la documentación u otra evidencia que demuestre que los custodios de claves han expresado su conocimiento de acuerdo con todos los elementos especificados en este requisito.	

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Brindar orientación a los clientes sobre cómo el transmitir, almacenar y actualizar claves criptográficas de manera segura puede contribuir a impedir que las claves se administren incorrectamente o se divulguen a entidades no autorizadas. **Información Adicional** En la Guía para los Requisitos 3.7.1-3.7.8. se citan diversas os estándares de la industria para la gestión de claves.
3.7.9 ***Requisito adicional sólo para proveedores de servicios:*** Cuando un proveedor de servicios comparte claves criptográficas con sus clientes para la transmisión o el almacenamiento de datos del tarjetahabiente, se documenta y distribuye a los clientes de los proveedores de servicios orientación sobre la transmisión, el almacenamiento y la actualización segura de dichas claves.	**3.7.9** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Si el proveedor de servicios comparte claves criptográficas con sus clientes para la transmisión o almacenamiento de datos de la cuenta, examínelos documentos que el proveedor de servicios proporciona a sus clientes para verificar que incluya orientación sobre cómo transmitir, almacenar y actualizar de forma segura las claves de los clientes de acuerdo con todos los elementos especificados en los Requisitos 3.7.1 a 3.7.8 anteriormente citados.	
Objetivo del Enfoque Personalizado		
Los clientes reciben una guía de administración de claves adecuada cada vez que reciben claves criptográficas compartidas.		
Notas de Aplicabilidad		
Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios.		

Requisito 4: Proteger los Datos de Tarjetahabientes con Criptografía Robusta Durante la Transmisión a través de Redes Abiertas y Públicas

Secciones	
4.1	Los procesos y mecanismos para proteger los datos de los titulares de tarjetas con criptografía sólida durante la transmisión a través de redes públicas abiertas están definidos y documentados.
4.2	Los PAN están protegidos con criptografía sólida durante la transmisión.

Descripción

El uso de criptografía sólida proporciona una mayor seguridad en la preservación de la confidencialidad, la integridad y el no repudio de los datos.

Para evitar ponerlos en peligro, los datos PAN deben estar cifrados durante la transmisión a través de redes a las que las personas malintencionadas pueden acceder fácilmente, incluidas las redes públicas y no confiables. Las redes inalámbricas mal configuradas y las vulnerabilidades en los protocolos de autenticación y cifrados heredados continúan siendo el objetivo de personas malintencionadas que buscan explotar estas vulnerabilidades para obtener acceso privilegiado a los entornos de datos de titulares de tarjetas (CDE). Cualquier transmisión de datos de titulares de tarjetas a través de la(s) red(es) interna(s) de una entidad naturalmente pondrá a esa red en el ámbito PCI DSS, ya que esa red almacena, procesa o transmite datos de titulares de tarjetas. Cualquiera de esas redes debe analizarse y examinarse según los requisitos aplicables PCI DSS.

El requisito 4 se aplica a las transmisiones de datos PAN a menos que se sea indicado específicamente en un requisito individual.

Las transmisiones datos PAN se pueden proteger cifrando los datos antes de que se transmitan, o cifrando la sesión sobre la cual se transmiten los datos, o ambos. Si bien no es necesario que se aplique una criptografía sólida tanto a nivel de datos como a nivel de la sesión, esta es una recomendación.

Consulte el Anexo G para conocer las definiciones de "criptografía sólida" y otros términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
4.1 Los procesos y mecanismos para proteger los datos de los titulares de tarjetas con criptografía sólida durante la transmisión a través de redes públicas abiertas están definidos y documentados.		
Requisitos del Enfoque Definido **4.1.1** Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 4 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la vigilancia en el cumplimiento con las actividades dentro del Requisito 4 están definidos y cumplidos por el personal afectado. Todas las actividades de apoyo son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.	**Procedimientos de Prueba del Enfoque Definido** **4.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 4 se gestionen de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** El Requisito 4.1.1 trata sobre la gestión y el mantenimiento eficiente de las diversas políticas y procedimientos especificados en el Requisito 4. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 4, es igualmente importante asegurarse de que estén debidamente documentados, mantenidos y difundidos. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocios. Por esta razón, considere actualizar estos documentos lo más pronto posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política. Las políticas y procedimientos, incluidas las actualizaciones, se comunican activamente a todo el personal involucrado y están respaldadas por procedimientos operativos que describen cómo realizar las actividades.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que las actividades críticas no se realicen. **Buenas Prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
4.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 4 están documentados, asignados y comprendidos.	**4.1.2.a** Evalúe la documentación para verificar que las descripciones de las funciones y las responsabilidades para realizar las actividades del Requisito 4 están documentadas y asignadas.	
	4.1.2.b Entreviste al personal responsable de desarrollar las actividades del Requisito 4 para verificar que los roles y responsabilidades se asignen según se documenten y sean entendidos.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 4. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
4.2 Los datos PAN está protegidos con criptografía sólida durante la transmisión.		
Requisitos del Enfoque Definido **4.2.1** Se implementan fuertes protocolos de seguridad y criptografía de la siguiente manera para proteger los datos PAN durante la transmisión a través de redes públicas abiertas: • Solo se aceptan claves y certificados confiables. • Los certificados utilizados para proteger los datos PAN durante la transmisión a través de redes públicas abiertas se confirman como válidos y no están vencidos ni revocados. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; consulte las notas de aplicabilidad a continuación para obtener más detalles.* • El protocolo en uso sólo admite versiones o configuraciones seguras y no admite el apoyo ni el uso de versiones, algoritmos, tamaños de clave o implementaciones inseguras. • La fuerza del cifrado es apropiada para la metodología de cifrado en uso. **Objetivo del Enfoque Personalizado** Los datos PAN de texto no cifrado no se pueden leer ni interceptar desde ninguna transmisión a través de redes públicas abiertas.	**Procedimientos de Prueba del Enfoque Definido** **4.2.1.a** Evalúe las políticas y procedimientos documentados y entreviste al personal para verificar que los procesos estén definidos para incluir todos los elementos especificados en este requisito. **4.2.1.b** Evalúe las configuraciones del sistema para verificar que se implementen protocolos de seguridad y criptografía sólida de acuerdo con todos los elementos especificados en este requisito. **4.2.1.c** Evalúe las transmisiones de datos de titulares de tarjetas para verificar que todos los datos PAN estén cifrados con criptografía sólida cuando se transmiten a través de redes públicas abiertas. **4.2.1.d** Evalúe las configuraciones del sistema para asegurarse de que se rechacen las claves y/o certificados que no se puedan verificar como confiables.	**Objetivo** La información confidencial debe cifrarse durante la transmisión a través de redes públicas ya que es fácil y común que individuos malintencionados intercepten y/o desvíen datos en tránsito. **Buenas Prácticas** Los diagramas de flujo de datos y de red definidos en el Requisito 1 constituyen recursos útiles para identificar todos los puntos de conexión donde se transmite o reciben datos de cuentas a través de redes públicas abiertas. Si bien no es obligatorio, se considera una buena práctica que las entidades también cifren los datos PAN en sus redes internas y que establezcan nuevas implementaciones de red con comunicaciones cifradas. Las transmisiones datos PAN se pueden proteger cifrando los datos antes de que se transmitan, o cifrando la sesión sobre la cual se transmiten los datos, o ambos. Si bien no es necesario que se aplique una criptografía sólida tanto a nivel de datos como a nivel de sesión, es altamente recomendado. Si se realiza un cifrado a nivel de datos, las claves criptográficas utilizadas se pueden administrar de acuerdo con los Requisitos 3.6 y 3.7 Si los datos están cifrados a nivel de la sesión, los custodios de claves designados deben tener la responsabilidad de gestionar las claves de transmisión y los certificados. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad		Algunas implementaciones de protocolo (como SSL, SSH v1.0 y TLS temprano) tienen vulnerabilidades conocidas que los atacantes pueden utilizar para obtener acceso a los datos en texto no cifrado. Es esencial que las entidades estén al tanto de las fechas de desactivación definidas por la industria para los conjuntos de cifrado que estén utilizando y se preparen para migrar a versiones o protocolos más nuevos cuando los más antiguos ya no se consideren seguros. Verificar que los certificados sean confiables ayuda a garantizar la integridad de la conexión segura. Para que se considere confiable, un certificado debe emitirse desde una fuente confiable, como una autoridad certificadora (CA) de confianza, y no debe estar vencido. Se pueden utilizar *Certificate Revocation Lists* (CRL) actualizadas u *Online Certificate Status Protocols* (OCSP) para validar los certificados. Las técnicas para validar certificados pueden incluir la fijación de certificados y claves públicas, donde el certificado de confianza o una clave pública se fija durante el desarrollo o en su primer uso. Las entidades también pueden confirmar con los desarrolladores o revisar el código fuente para asegurarse de que los clientes y servidores rechacen las conexiones si el certificado es incorrecto. Para los certificados TLS basados en navegador, la confiabilidad del certificado a menudo se puede verificar haciendo clic en el icono de candado que aparece junto a la barra de direcciones. *(continúa en la página siguiente)*
Puede haber casos en los que una entidad reciba datos de titulares de tarjetas no solicitados a través de un canal de comunicación inseguro que no fue diseñado con el propósito de recibir datos confidenciales. Ante esta situación, la entidad puede optar por incluir el canal en su CDE y asegurarlo de acuerdo con PCI DSS o implementar medidas para impedir que el canal se utilice para datos de titulares de tarjetas. Un certificado auto-firmado también puede ser aceptable si el certificado es emitido por una CA interna dentro de la organización, si el autor del certificado está confirmado y si el certificado está verificado (por ejemplo, mediante *hash* o firma) y no está caducado. Hay que tomar en cuenta que los certificados auto-firmados en los que en el campo de Denominación Distinguida (DN) bajo "emitido por" y "emitido para" aparece la misma información, no son aceptables. *El punto anterior (para confirmar que los certificados utilizados para proteger los datos PAN durante la transmisión a través de redes públicas abiertas son válidos y no están vencidos ni revocados) es una mejor práctica hasta el 31 de marzo de 2025, después de lo cual se requerirá como parte del Requisito 4.2.1 y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
		Ejemplos Las redes públicas abiertas incluyen, entre otras: • El Internet y • Tecnologías inalámbricas, incluidas Wi-Fi, Bluetooth, tecnologías celulares y comunicaciones por satélite. **Información Adicional** Se pueden consultar las recomendaciones de los proveedores y las mejores prácticas de la industria para obtener información acerca de la solidez adecuada del cifrado específica para la metodología de cifrado que se esté utilizando. Para obtener más información sobre criptografía sólida y protocolos seguros, consulte los estándares de la industria y las mejores prácticas, como *NIST SP 800-52 y SP 800-57.* Para obtener más información sobre claves y certificados confiables, consulte la *Publicación Especial de la Guía Práctica de Ciberseguridad del NIST1800-16, Protección de Transacciones Web: Gestión de Certificados del Servidor de Seguridad de la Capa de Transporte (TLS).*

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
4.2.1.1 Se mantiene un inventario de las claves y certificados confiables de la entidad utilizados para proteger los datos PAN durante la transmisión.	**4.2.1.1.a** Evalúe las políticas y los procedimientos documentados para verificar que los procesos estén definidos para que la entidad mantenga un inventario de sus claves y certificados confiables.	El inventario de claves confiables ayuda a la entidad a realizar un seguimiento de los algoritmos, los protocolos, la solidez de las claves, los custodios de claves y las fechas de caducidad de las claves. Esto permite que la entidad responda rápidamente a las vulnerabilidades descubiertas en el software de cifrado, los certificados y los algoritmos criptográficos.
Objetivo del Enfoque Personalizado	**4.2.1.1.b** Evalúe el inventario de claves y certificados confiables para verificar que se mantenga actualizado.	**Buenas Prácticas**
Todas las claves y certificados utilizados para proteger los datos PAN durante la transmisión se identifican y confirman como confiables.		Para los certificados, el inventario debe incluir la CA emisora y la fecha de caducidad de la certificación.
Notas de Aplicabilidad		
Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **4.2.1.2** Las redes inalámbricas que transmiten datos PAN o están conectadas al CDE utilizan las mejores prácticas de la industria para implementar criptografía sólida para autenticación y transmisión. **Objetivo del Enfoque Personalizado** Los datos PAN no cifrados no se pueden leer ni interceptar en las transmisiones de la red inalámbrica.	**Procedimientos de Prueba del Enfoque Definido** **4.2.1.2** Evalúe las configuraciones del sistema para verificar que las redes inalámbricas que transmiten datos PAN o están conectadas al CDE utilizan las mejores prácticas de la industria para implementar criptografía sólida para autenticación y transmisión.	**Objetivo** Dado que las redes inalámbricas no requieren medios físicos para conectarse, es importante establecer controles que limiten quién puede conectarse y qué protocolos de transmisión se utilizarán. Usuarios malintencionados utilizan herramientas gratuitas y ampliamente disponibles para espiar las comunicaciones inalámbricas. El uso de una criptografía sólida puede ayudar a limitar la divulgación de información confidencial a través de redes inalámbricas. Las redes inalámbricas presentan riesgos únicos para una organización; por lo tanto, deben identificarse y protegerse de acuerdo con los requisitos de la industria. Se requiere una criptografía sólida para la autenticación y transmisión de datos PAN para impedir que usuarios malintencionados obtengan acceso a la red inalámbrica o utilicen redes inalámbricas para acceder a otras redes o datos internos. **Buenas Prácticas** Las redes inalámbricas no deben permitir el retroceso o la degradación a un protocolo inseguro o a un nivel de cifrado más bajo que no cumpla con la intención de la criptografía sólida. **Información Adicional** Revise la documentación específica del proveedor para obtener más detalles sobre la elección de protocolos, configuraciones y ajustes relacionados con la criptografía.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
4.2.2 Los datos PAN están protegidos con criptografía sólida siempre que se envíen a través de tecnologías de mensajería para el usuario final.	**4.2.2.a** Evalúe las políticas y procedimientos documentados para verificar que los procesos estén definidos para asegurar os datos PAN con criptografía sólida siempre que se envíen a través de tecnologías de mensajería de usuario final.	Las tecnologías de mensajería para el usuario final normalmente se pueden interceptar fácilmente mediante la detección de paquetes durante la entrega a través de redes internas y públicas. **Buenas Prácticas** El uso de la tecnología de mensajería del usuario final para enviar datos PAN solo debe considerarse cuando existe una necesidad de negocio definida. **Ejemplos** Los correos electrónicos, la mensajería instantánea, los SMS y el chat son ejemplos del tipo de tecnología de mensajería para el usuario final al que se refiere este requisito.
Objetivo del Enfoque Personalizado Los datos PAN de texto no cifrado no se pueden leer ni interceptar de las transmisiones que utilizan tecnologías de mensajería para el usuario final.	**4.2.2.b** Evalúe las configuraciones del sistema y la documentación del proveedor para verificar que los datos PAN esté protegidos con criptografía sólida siempre que se envíe a través de tecnologías de mensajería para el usuario final.	
Notas de Aplicabilidad Este requisito también se aplica si un cliente u otro tercero solicitan que se le envíen datos PAN a través de tecnologías de mensajería para el usuario final. Puede haber casos en los que una entidad reciba datos de titulares de tarjetas no solicitados a través de un canal de comunicación inseguro que no está destinado a la transmisión de datos confidenciales. Ante esta situación, la entidad puede optar por incluir el canal en su CDE y asegurarlo de acuerdo con PCI DSS o borrar los datos del tarjetahabiente e implementar medidas para impedir que el canal se utilice para datos de titulares de tarjetas.		

Mantener un Programa de Gestión de Vulnerabilidades

Requisito 5: Proteger Todos los Sistemas y Redes de Software Malicioso

Secciones	
5.1	Se definen y comprenden los procesos y mecanismos para proteger todos los sistemas y redes del software malintencionado.
5.2	El software malintencionado (malware) es evadido, o se detecta y se soluciona.
5.3	Los mecanismos y procesos antivirus están activos, mantenidos y monitoreados.
5.4	Los mecanismos contra el *phishing* protegen a los usuarios contra los ataques de fraude informático.

Descripción

El software malicioso (malware) es un software o firmware diseñado para infiltrarse o dañar un sistema informático sin el conocimiento o el consentimiento del propietario, con la intención de comprometer la confidencialidad, la integridad o la disponibilidad de los datos del propietario, las aplicaciones o el sistema operativo.

Algunos ejemplos de ello son virus, gusanos, troyanos, software espía (spyware), software secuestrador *(ransomware), keyloggers y rootkits*, código malicioso, *scripts* y enlaces.

El software malicioso puede entrar en la red durante muchas actividades aprobadas por la empresa, incluyendo el correo electrónico de los empleados (por ejemplo, a través del *phishing)* y el uso de Internet, los ordenadores móviles y los dispositivos de almacenamiento, lo que resulta en la explotación de las vulnerabilidades del sistema.

El uso de soluciones *antimalware* que abordan todos los tipos de malware ayuda a proteger los sistemas de las amenazas de malware actuales y en progreso.

Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
5.1 Se definen y comprenden los procesos y mecanismos para proteger todos los sistemas y redes del software malicioso.		
Requisitos del Enfoque Definido **5.1.1** Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 5 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la vigilancia en el cumplimiento con las actividades dentro del Requisito 5 están definidos y cumplidos por el personal afectado. Todas las actividades de apoyo se pueden repetir de forma coherente y deben ajustarse a las intenciones de la dirección.	**Procedimientos de Prueba del Enfoque Definido** **5.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 5 son administrados de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** El requisito 5.1.1 trata sobre la gestión y el mantenimiento eficiente de las distintas políticas y procedimientos especificados a lo largo del Requisito 5. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 5, es igualmente importante garantizar que se documenten, se mantengan y se difundan adecuadamente. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocios. Por esta razón, considere actualizar estos documentos lo más pronto posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
5.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 5 están documentados, asignados y comprendidos.	**5.1.2.a** Evalúe la documentación para verificar que las descripciones de las funciones y las responsabilidades para realizar las actividades del Requisito 5 están documentadas y asignadas.	Si los roles y las responsabilidades no se asignan formalmente, es posible que las redes y los sistemas no estén adecuadamente protegidos contra el malware. **Buenas Prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
Objetivo del Enfoque Personalizado	**5.1.2.b** Entreviste al personal responsable de desarrollar las actividades del Requisito 5 para verificar que los roles y responsabilidades se asignen según sean documentadas y entendidas.	
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 5. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
5.2 El software malintencionado (malware) es evadido, o se detecta y se soluciona.		
Requisitos del Enfoque Definido **5.2.1** Una solución antimalware se aplicará a todos los componentes del sistema, excepto a aquellos componentes del sistema identificados en evaluaciones periódicas según el Requisito 5.2.3 que concluye que los componentes del sistema no están en riesgo de malware. **Objetivo del Enfoque Personalizado** Se implementan mecanismos automatizados para impedir que los sistemas se conviertan en un vector de ataque para el malware.	**Procedimientos de Prueba del Enfoque Definido** **5.2.1.a** Evalúe los componentes del sistema para verificar que se implemente una solución antimalware en todos ellos, excepto aquellos en los que se determine que no están en riesgo de malware según las evaluaciones periódicas del Requisito 5.2.3. **5.2.1.b** Para cualquier componente del sistema que no cuente con una solución antimalware, analice las evaluaciones periódicas para verificar que el componente fue evaluado y que la conclusión de la evaluación es que el componente no está en riesgo de malware.	**Objetivo** Existe un flujo constante de ataques dirigidos a vulnerabilidades recién descubiertas en sistemas que antes se consideraban seguros. Sin una solución antimalware que se actualice regularmente, pueden aparecer nuevas formas de malware para atacar los sistemas, deshabilitar una red o comprometer datos. **Buenas Prácticas** Es beneficioso para las entidades estar al tanto de los ataques de "día cero" (aquellos que explotan una vulnerabilidad previamente desconocida) y considerar soluciones que se enfoquen en las características del comportamiento y que alertarán y reaccionarán ante un comportamiento inesperado. **Definiciones** Los componentes del sistema que se sabe que están afectados por malware tienen ataques de malware activos disponibles en el mundo real (no solo ataques teóricos).

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Es importante protegerse contra todo tipo y forma de malware y así impedir el acceso no autorizado. **Buenas Prácticas** Las soluciones antimalware pueden incluir una combinación de controles basados en la red, controles basados en el hosts y soluciones de seguridad para terminales. Además de las herramientas basadas en firmas, las capacidades utilizadas por las soluciones antimalware modernas incluyen la caja de arena, controles de escalamiento de privilegios y aprendizaje automático. Las técnicas de solución incluyen impedir que el malware ingrese a la red y eliminar o contener malware que ingrese a la red. **Ejemplos** Los tipos de malware incluyen, entre otros, virus, troyanos, gusanos, software espía, software secuestrador *ransomware, keyloggers, rootkits,* código malicioso, scripts y enlaces.
5.2.2 Las soluciones antimalware implementadas: • Detectan todos los tipos conocidos de malware. • Eliminan, bloquean o contienen todos los tipos conocidos de malware.	**5.2.2** Evalúe la documentación del proveedor y las configuraciones de las soluciones antimalware para verificar que la solución: • Detecta todos los tipos conocidos de malware. • Elimina, bloquean o contienen todos los tipos conocidos de malware.	
Objetivo del Enfoque Personalizado		
El malware no puede ejecutar o infectar otros componentes del sistema.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
5.2.3 Todos los componentes del sistema que no se encuentren en riesgo de malware se evalúan periódicamente para incluir lo siguiente: • Una lista documentada de todos los componentes del sistema que no están en riesgo de malware. • Identificación y evaluación de amenazas de malware en evolución para los componentes del sistema. • Confirmación de si dichos componentes del sistema continúan sin requerir protección antimalware.	**5.2.3.a** Evalúe las políticas y los procedimientos documentados para verificar que se haya definido un proceso para las evaluaciones periódicas de cualquier componente del sistema que no esté en riesgo de malware que incluya todos los elementos especificados en este requisito. **5.2.3.b** Entreviste al personal para verificar que las evaluaciones incluyen todos los elementos especificados en este requisito. **5.2.3.c** Evalúe la lista de componentes del sistema identificados como sin riesgo de malware y compararlos con los componentes del sistema sin una solución antimalware implementada según el Requisito 5.2.1 para verificar que los componentes del sistema coincidan con ambos requisitos.	Es posible que algunos sistemas, en un momento dado, no sean objetivos frecuentes o afectados por malware. Sin embargo, las tendencias de la industria en materia de malware pueden cambiar rápidamente, por lo que es importante que las organizaciones estén al tanto de los nuevos programas maliciosos que podrían afectar sus sistemas, por ejemplo, monitoreando los avisos de seguridad de los proveedores y los foros antimalware para determinar si sus sistemas podrían estar fallando. **Buenas Prácticas** Si una entidad determina que un sistema en particular no es susceptible a ningún malware, dicha determinación debe estar respaldada por evidencia de la industria, recursos de proveedores y mejores prácticas. Los siguientes pasos pueden ayudar a las entidades durante sus evaluaciones periódicas: • Identificación de todos los tipos de sistemas para los que se determinó previamente que no requieren protección contra malware. • Revisión de alertas y avisos de vulnerabilidad de la industria para determinar si existen nuevas amenazas para cualquier sistema identificado. • Una conclusión documentada acerca de si los tipos de sistema siguen siendo susceptibles al malware. • Una estrategia para agregar protección contra malware para cualquier tipo de sistema para el que la protección contra malware se haya vuelto necesaria. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado		
La entidad es consciente de la evolución de las amenazas de malware para garantizar que los sistemas que no estén protegidos contra el malware no corran riesgo de infección.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Los componentes del sistema cubiertos por este requisito son aquellos para los que no existe una solución antimalware implementada según el Requisito 5.2.1.		Las tendencias en tipos de malware deben incluirse en la identificación de nuevas vulnerabilidades de seguridad en el Requisito 6.3.1, y los métodos para abordar las nuevas tendencias deben incorporarse en los estándares de configuración de la entidad y los mecanismos de protección según sea necesario.
Requisitos del Enfoque Definido **5.2.3.1** La frecuencia de las evaluaciones periódicas de los componentes del sistema identificados como no en riesgo de malware se define en el análisis de riesgo específico de la entidad, el cual se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1.	**Procedimientos de Prueba del Enfoque Definido** **5.2.3.1.a** Evalúe el análisis de riesgo específico de la entidad para conocer la frecuencia de las evaluaciones periódicas de los componentes del sistema identificados como no en riesgo de malware para verificar que el análisis de riesgo se realizó de acuerdo con todos los elementos especificados en el Requisito 12.3. 1. **5.2.3.1.b** Evalúe los resultados documentados de las evaluaciones periódicas de los componentes del sistema identificados como no en riesgo de malware y entreviste al personal para verificar que las evaluaciones se realicen con la frecuencia definida en el análisis de riesgo específico de la entidad realizado para este requisito.	**Objetivo** Las entidades determinan el período óptimo para realizar la evaluación basándose en criterios como la complejidad del entorno de cada entidad y la cantidad de tipos de sistemas que se requiere examinar.
Objetivo del Enfoque Personalizado Los sistemas que no se sabe que están en riesgo de malware se reevalúan con una frecuencia que considere el nivel de riesgo de la entidad.		
Notas de Aplicabilidad *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
5.3 Los mecanismos y procesos antimalware están activos, mantenidos y monitoreados.		
Requisitos del Enfoque Definido **5.3.1** Las soluciones antimalware se mantienen actualizadas a través de procesos de actualización automáticos. **Objetivo del Enfoque Personalizado** Los mecanismos antimalware pueden detectar y abordar las últimas amenazas de malware.	**Procedimientos de Prueba del Enfoque Definido** **5.3.1.a** Evalúe las configuraciones de las soluciones antimalware, incluyendo cualquier instalación maestra del software, para verificar que la solución esté configurada para realizar actualizaciones automáticas. **5.3.1.b** Evalúe los componentes y los registros del sistema para verificar que las soluciones y las definiciones antimalware estén actualizadas y se hayan implementado de inmediato.	**Objetivo** Para que una solución antimalware siga siendo efectiva, necesita tener las últimas actualizaciones de seguridad, firmas, motores de análisis de amenazas y cualquier otra protección contra malware en la que se base la solución. Tener un proceso de actualización automatizado evita sobrecargar a los usuarios finales con la responsabilidad de instalar actualizaciones manualmente y proporciona una mayor garantía de que los mecanismos de protección antimalware se actualizan lo más rápido posible después de que se lanza una actualización. **Buenas Prácticas** Los mecanismos antimalware deben actualizarse a través de una fuente confiable tan pronto como sea posible después de que exista una nueva actualización disponible. El uso de una fuente común confiable para distribuir actualizaciones a los sistemas de los usuarios finales ayuda a garantizar la integridad y coherencia de la arquitectura de la solución. Las actualizaciones se pueden descargar automáticamente a una ubicación central, por ejemplo, para permitir las pruebas, antes de implementarlas en los componentes individuales del sistema.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
5.3.2 Soluciones antimalware: • Realizan escaneos periódicos y escaneos activos o en tiempo real. **O** • Realizan un análisis continuo del comportamiento de los sistemas o procesos.	**5.3.2.a** Evalúe las configuraciones de las soluciones antimalware, incluyendo cualquier instalación maestra del software, para comprobar que la solución o soluciones están configuradas para realizar al menos uno de los elementos especificados en este requisito.	**Objetivo** El escaneo periódico puede identificar malware que está presente en el entorno, pero temporalmente inactivo. Algunos programas maliciosos, como el malware de día cero, pueden ingresar a un entorno antes de que la solución de escaneo sea capaz de detectarlos. Realizar escaneos periódicos regulares o análisis de comportamiento continuo de los sistemas o procesos ayuda a garantizar que el malware previamente indetectable, se pueda identificar, eliminar e investigar para determinar cómo obtuvo acceso al entorno. **Buenas Prácticas** El uso de una combinación de escaneos periódicos (programados y a la carta) y escaneos activos en tiempo real (al momento del acceso), ayuda a garantizar que se aborde el malware que reside en los elementos estáticos y dinámicos del CDE. Los usuarios también deberían poder ejecutar escaneos en sus sistemas bajo demanda si se detecta actividad sospechosa - esto puede ser útil para la detección temprana de malware. Los escaneos deben incluir todo el sistema de archivos, incluyendo todos los discos, la memoria y los archivos de inicio y los registros de arranque (al reiniciar el sistema) para detectar todo el malware al ejecutar los archivos, incluyendo cualquier software que pueda residir en un sistema pero que no esté activo en ese momento. El alcance del escaneo debe incluir todos los sistemas y el software del CDE, incluidos los que a menudo se pasan por alto, como los servidores de correo electrónico, los navegadores web y el software de mensajería instantánea. *(continúa en la página siguiente)*
	5.3.2.b Evalúe los componentes del sistema, incluyendo todos los tipos de sistemas operativos identificados como riesgo de malware, para verificar que las soluciones están habilitadas de acuerdo con al menos uno de los elementos especificados en este requisito.	
	5.3.2.c Evalúe los registros y los resultados de lo escaneo para verificar que las soluciones están habilitadas de acuerdo con al menos uno de los elementos especificados en este requisito.	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado El malware no puede completar la ejecución.		**Definiciones** El escaneo activo, o en tiempo real, comprueba los archivos en busca de malware ante cualquier intento de abrir, cerrar, renombrar o interactuar de otra manera con un archivo, impidiendo que el malware se active.
Requisitos del Enfoque Definido **5.3.2.1** Si se realizan escaneos periódicos de malware para cumplir con el requisito 5.3.2, la frecuencia de los escaneos se define en el análisis de riesgos específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1.	**Procedimientos de Prueba del Enfoque Definido** **5.3.2.1.a** Evalúe el análisis de riesgos específico de la entidad para la frecuencia de los escaneos periódicos de malware a fin de verificar que el análisis de riesgos se realizó de acuerdo con todos los elementos especificados en el Requisito 12.3.1. **5.3.2.1.b** Evalúe los resultados documentados de los escaneos periódicos de malware y entreviste al personal para verificar que los escaneos se realicen con la frecuencia definida en el análisis de riesgo específico de la entidad realizado para este requisito.	**Objetivo** Las entidades pueden determinar el período óptimo para llevar a cabo escaneos periódicos por ellos mismos basados en su propia evaluación de los riesgos presentes en sus entornos.
Objetivo del Enfoque Personalizado Los escaneos realizados por la solución de malware se llevan a cabo con una frecuencia que se ajusta al riesgo de la entidad.		
Notas de Aplicabilidad Este requisito aplica para las entidades que realizan escaneos periódicos de malware para cumplir con el Requisito 5.3.2. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
5.3.3 Para los medios electrónicos extraíbles, la solución antimalware: • Realiza escaneos automáticos cuando el medio es insertado, conectado o montado lógicamente, **O** • Realiza un análisis continuo del comportamiento de los sistemas o procesos cuando el medio está insertado, conectado o montado lógicamente.	**5.3.3.a** Evalúe las configuraciones de las soluciones antimalware para verificar que, en el caso de los medios electrónicos extraíbles, la solución está configurada para realizar al menos uno de los elementos especificados en este requisito.	Los dispositivos multimedia portátiles suelen pasarse por alto como método de entrada de malware. Los atacantes suelen precargar el malware en dispositivos portátiles como USB y memorias flash; al conectar un dispositivo infectado a un ordenador se activa el malware, introduciendo nuevas amenazas en el entorno.
	5.3.3.b Evalúe los componentes del sistema con medios electrónicos extraíbles conectados para verificar que la solución o soluciones están habilitadas de acuerdo con al menos uno de los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado	**5.3.3.c** Evalúe los registros y resultados de los escaneos para verificar que las soluciones están habilitadas de acuerdo con al menos uno de los elementos especificados en este requisito.	
El malware no puede introducirse en los componentes del sistema a través de medios extraíbles externos.		
Notas de Aplicabilidad		
Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Es importante hacer un seguimiento de la eficacia de los mecanismos antimalware, por ejemplo, confirmando que las actualizaciones y los escaneos se realizan como esperado, y que el malware se identifica y es abordado. Los registros de auditoría también permiten a una entidad determinar cómo entró el malware en su entorno y continuar con sus actividades cuando está dentro de la red de la entidad.
5.3.4 Los registros de auditoría de la solución antimalware están habilitados y se conservan de acuerdo con el requisito 10.5.1.	**5.3.4** Evalúe las configuraciones de la solución antimalware para comprobar que los registros están activados y se conservan de acuerdo con el Requisito 10.5.1.	
Objetivo del Enfoque Personalizado		
Los registros históricos de las acciones antimalware están disponibles inmediatamente y se conservan durante al menos 12 meses.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Es importante que los mecanismos defensivos estén siempre en funcionamiento para que el malware se detecte en tiempo real. La activación y desactivación ad hoc de las soluciones antimalware podrían permitir que los programas maliciosos se propaguen sin control y sin ser detectados. **Buenas Prácticas** Cuando exista una necesidad legítima de desactivar temporalmente la protección antimalware de un sistema -por ejemplo, para apoyar una actividad específica de mantenimiento o la investigación de un problema técnico-, la razón para tomar tal acción debe ser entendida y aprobada por un gerente apropiado. Cualquier desactivación o alteración de los mecanismos antimalware, incluso en los propios dispositivos de los administradores, debe ser realizada por personal autorizado. Se reconoce que los administradores tienen privilegios que pueden permitirles desactivar el antimalware en sus propios ordenadores, pero deben existir mecanismos de alerta cuando se desactiva dicho software y luego realizar un seguimiento para garantizar que se han seguido los procesos correctos. **Ejemplos** Entre las medidas de seguridad adicionales que podrían aplicarse durante el periodo en el que la protección antimalware no está activa, se incluye la desconexión del sistema desprotegido de Internet mientras la protección antimalware está desactivada y la ejecución de un análisis completo una vez que se vuelva a activar.
5.3.5 Los mecanismos antimalware no pueden ser desactivados o alterados por los usuarios, a menos que esté específicamente documentado y autorizado por la administración en cada caso, por un período de tiempo limitado.	**5.3.5.a** Evalúe las configuraciones antimalware, para verificar que los mecanismos antimalware no pueden ser deshabilitados o alterados por los usuarios.	
Objetivo del Enfoque Personalizado Los mecanismos antimalware no pueden ser modificados por personal no autorizado.	**5.3.5.b** Entreviste al personal responsable y observe los procesos para verificar que cualquier solicitud de desactivación o alteración de los mecanismos antimalware esté específicamente documentada y autorizada por la dirección, caso por caso y por un período de tiempo limitado.	
Notas de Aplicabilidad Las soluciones antimalware sólo pueden desactivarse temporalmente si existe una necesidad técnica legítima, autorizada por la dirección en cada caso. Si es necesario desactivar la protección antimalware para un fin específico, esto debe ser formalmente autorizado. También puede ser necesario implementar medidas de seguridad adicionales para el período durante el cual la protección antimalware no está activa.		

Requisitos y Procedimientos de Prueba		Guía
5.4 Los mecanismos contra *phishing* protegen a los usuarios contra los ataques de *phishing.*		
Requisitos del Enfoque Definido **5.4.1** Existen procesos y mecanismos automatizados para detectar y proteger al personal contra ataques de *phishing.* **Objetivo del Enfoque Personalizado** Existen mecanismos para proteger y mitigar el riesgo que plantean los ataques de *phishing.* **Notas de Aplicabilidad** Este requisito se aplica al mecanismo automatizado. No se pretende que los sistemas y servicios que proporcionan tales mecanismos automatizados (como servidores de correo electrónico) entren en el ámbito PCI DSS. El enfoque de este requisito es proteger al personal con acceso a los componentes del sistema en el ámbito PCI DSS. Cumplir con este requisito de controles técnicos y automatizados para detectar y proteger al personal contra el *phishing* no es igual a lo que establece el Requisito 12.6.3.1 en cuanto al entrenamiento de concienciación sobre seguridad. Cumplir con este requisito tampoco implica que se está cumpliendo con el requisito de proporcionar al personal capacitación en cuanto a concienciación de seguridad, y viceversa. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba del Enfoque Definido** **5.4.1** Observe los procesos y mecanismos implementados para verificar que se hayan instalado controles para detectar y proteger al personal contra ataques de *phishing.*	**Objetivo** Los controles técnicos pueden limitar la cantidad de ocasiones que el personal tiene para examinar la veracidad de una comunicación y también pueden limitar los efectos de las respuestas individuales al *phishing.* **Buenas Prácticas** Al desarrollar controles contra el *phishing*, se anima a las entidades a considerar una combinación de enfoques. Por ejemplo, el uso de controles *anti-spoofing* como Autenticación de mensajes basada en dominio, Informes y conformidad (DMARC), Marco de Políticas del Remitente (SPF) y Correo Identificado con Claves de Dominio (DKIM) ayudará a evitar que los *phishers* falsifiquen el dominio de la entidad y se hagan pasar por personal. La implementación de tecnologías para bloquear correos electrónicos de *phishing* y malware antes de que lleguen al personal, como depuradores de enlaces y antimalware del lado del servidor, puede reducir los incidentes y disminuir el tiempo requerido por el personal para verificar e informar ataques de *phishing.* Además, capacitar al personal para reconocer y reportar los correos electrónicos de *phishing* puede permitir que se identifiquen correos electrónicos similares y que se eliminen antes de abrirlos. Se recomienda (pero no es obligatorio) que se apliquen controles *anti-phishing* en toda la organización de una entidad. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
		Definiciones El *phishing* es una forma de ingeniería social y describe los diferentes métodos utilizados por los atacantes para engañar al personal para que revele información confidencial, como nombres de cuentas de usuario y contraseñas, y datos de cuentas. Los atacantes generalmente se disfrazarán e intentarán aparecer como una fuente genuina o confiable, indicando al personal que envíe una respuesta por correo electrónico, haga clic en un enlace web o ingrese datos en un sitio web comprometido. Los mecanismos que pueden detectar e impedir intentos de *phishing* a menudo se incluyen en las soluciones antimalware. **Información Adicional** Consulte lo siguiente para obtener más información sobre la suplantación de identidad *(phishing):* *Centro Nacional de Seguridad Cibernética - Ataques de phishing: Defendiendo su Organización.* *Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU.: Informe de sitios de phishing.*

Requisito 6: Desarrollar y Mantener Sistemas y Softwares Seguros

Secciones	
6.1	Se definen y comprenden los procesos y mecanismos para desarrollar y mantener sistemas y software seguros.
6.2	El software a medida y personalizado se desarrolla de forma segura.
6.3	Las vulnerabilidades de seguridad se identifican y son abordadas.
6.4	Las aplicaciones web públicas están protegidas contra ataques.
6.5	Los cambios en todos los componentes del sistema se gestionan de forma segura.

Descripción

Los actores con malas intenciones pueden utilizar las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades son solucionadas por parches de seguridad proporcionados por el proveedor, los cuales deben ser instalados por las entidades que administran los sistemas. Todos los componentes del sistema deben tener todos los parches de software apropiados para proteger contra la explotación y la puesta en riesgo de los datos del tarjetahabiente por parte de personas y software malintencionado.

Los parches de software apropiados son aquellos parches que han sido suficientemente evaluados y probados para determinar que no entran en conflicto con las configuraciones de seguridad existentes. Al software a medida y personalizado, se le pueden evitar numerosas vulnerabilidades aplicando procesos de ciclo de vida del software (SLC) y técnicas de codificación segura.

Los repositorios de código que almacenan el código de la aplicación, las configuraciones del sistema u otros datos de configuración que podrían afectar la seguridad de los datos de cuentas o del CDE, están dentro del alcance de las evaluaciones PCI DSS.

Consulte la Relación entre los estándares de software PCI DSS y PCI SSC en la página 8 para obtener información sobre el uso de software validado por PCI SSC y los proveedores de software, y cómo el uso de los estándares de software PCI SCC puede ayudar a cumplir con los controles del Requisito 6.

Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

***Nota**: El requisito 6 se aplica a todos los componentes del sistema, a excepción de la sección 6.2 para el desarrollo de software de forma segura, el cual aplica sólo al software a medida y personalizado utilizado en cualquier componente del sistema incluido o conectado al CDE.*

Requisitos y Procedimientos de Prueba		Guía
6.1 Se definen y comprenden los procesos y mecanismos para desarrollar y mantener sistemas y software seguros.		
Requisitos del Enfoque Definido **6.1.1** Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 6 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la vigilancia en el cumplimiento con las actividades dentro del Requisito 6 están definidos y cumplidos por el personal afectado. Todas las actividades de apoyo son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.	**Procedimientos de Prueba del Enfoque Definido** **6.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 6 son administrados de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** El Requisito 6.1.1 trata sobre la gestión y el mantenimiento eficiente de las diversas políticas y procedimientos especificados en el Requisito 6. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 6, es igualmente importante garantizar que se documenten, se mantengan y se difundan adecuadamente. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocios. Por esta razón, considere actualizar estos documentos lo más pronto posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Si los roles y responsabilidades no se asignan formalmente, los sistemas no se mantendrán de manera segura y su nivel de seguridad se reducirá. **Buenas Prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
6.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 6 están documentadas, asignadas y comprendidas.	**6.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y responsabilidades para realizar las actividades del Requisito 6 estén documentadas y asignadas.	
	6.1.2.b Entreviste al personal responsable de realizar las actividades del Requisito 6 para verificar que los roles y responsabilidades se asignan según se documenta y se entienden.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 6. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
6.2 El software a medida y personalizado se desarrolla de forma segura.		
Requisitos del Enfoque Definido **6.2.1** El software a medida y personalizado se desarrolla de forma segura, de la siguiente manera: • Basándose en estándares de la industria y/o mejores prácticas para un desarrollo seguro. • De acuerdo con PCI DSS (por ejemplo, autenticación segura y registro). • Considerando la incorporación de la información de problemas de seguridad durante cada etapa del ciclo de vida del desarrollo de software. **Objetivo del Enfoque Personalizado** El software a medida y personalizado se desarrolla de acuerdo con PCI DSS y procesos de desarrollo seguros durante todo el ciclo de vida del software. **Notas de Aplicabilidad** Esto se aplica a todo el software desarrollado por o para la entidad para su propio uso. Esto incluye software tanto a la medida como personalizado. Esto no aplica para el software de terceros.	**Procedimientos de Prueba del Enfoque Definido** **6.2.1** Evalúe los procedimientos de desarrollo de software documentados para verificar que los procesos están definidos y que incluyen todos los elementos especificados en este requisito.	**Objetivo** Sin la inclusión de la seguridad durante las fases de definición, diseño, análisis y prueba de los requisitos del desarrollo de software, las vulnerabilidades de seguridad pueden introducirse de forma inadvertida o maliciosa en el entorno de producción. **Buenas Prácticas** Comprender cómo la aplicación maneja los datos confidenciales, incluso cuando se almacenan, transmiten y están en la memoria, puede ayudar a identificar dónde se deben proteger los datos. Los requisitos de PCI DSS deben tenerse en cuenta al desarrollar el software para cumplir con ellos desde el diseño, en lugar de intentar actualizar el software más adelante. **Ejemplos** Las metodologías y marcos de gestión del ciclo de vida del software seguro incluyen el marco PCI de Software Seguro, BSIMM, OPENSAMM, y elaboradas desde NIST, ISO y SAFECode.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Tener personal con conocimientos en métodos de codificación segura, incluidas las técnicas definidas en el Requisito 6.2.4, ayudará a minimizar el número de vulnerabilidades de seguridad introducidas a través de prácticas de codificación deficientes. **Buenas Prácticas** La formación para desarrolladores puede proveerse internamente o por terceros. La capacitación debe incluir, entre otros, lenguajes de desarrollo en uso, diseño de software seguro, técnicas de codificación segura, uso de técnicas/métodos para encontrar vulnerabilidades en los códigos, procesos para impedir la reintroducción de vulnerabilidades previamente resueltas y cómo utilizar cualquier herramienta de pruebas de seguridad automatizada para detectar vulnerabilidades en el software. A medida que cambian las prácticas de codificación segura aceptadas por la industria, es posible que sea necesario actualizar las prácticas de codificación organizacional y la capacitación de los desarrolladores para abordar nuevas amenazas.
6.2.2 El personal de desarrollo de software que trabaja en software a medida y personalizado recibe capacitación al menos una vez cada 12 meses de la siguiente manera: • Sobre la seguridad del software relevante para su función laboral y lenguajes de desarrollo. • Incluyendo diseño de software seguro y técnicas de codificación segura. • Incluyendo, si se utilizan herramientas de prueba de seguridad, cómo utilizar las herramientas para detectar vulnerabilidades en el software.	**6.2.2.a** Evalúe los procedimientos de desarrollo de software para verificar que los procesos estén definidos para capacitar al personal de desarrollo de software para que desarrolle software a medida y personalizado que incluya todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado	**6.2.2.b** Evalúe los registros de capacitación y entreviste al personal para verificar que el personal de desarrollo de software que trabaja en software a medida y personalizado haya recibido capacitación en seguridad de software que sea relevante para su función laboral y lenguajes de desarrollo de acuerdo con todos los elementos especificados en este requisito.	
El personal de desarrollo de software sigue estando informado sobre las prácticas de desarrollo seguras; seguridad de software; y ataques contra los lenguajes, marcos o aplicaciones que desarrollan. El personal puede recibir asistencia y orientación cuando sea necesario.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
6.2.3 El software a medida y personalizado es revisado antes de ser lanzado a producción o para los clientes, a fin de identificar y corregir posibles vulnerabilidades de codificación, de la siguiente manera: • Las revisiones de código garantizan que el código se desarrolle de acuerdo con las pautas de codificación segura. • Las revisiones de código buscan vulnerabilidades de software tanto existente como emergente. • Las correcciones apropiadas se implementan antes de la publicación.	**6.2.3.a** Evalúe los procedimientos de desarrollo de software documentados y entreviste al personal responsable para verificar que los procesos están definidos y requieren que todo el software personalizado y personalizado sea revisado de acuerdo con todos los elementos especificados en este requisito. **6.2.3.b** Evalúe la evidencia de los cambios en el software a medida y personalizado para verificar que los cambios en el código se revisaron de acuerdo con todos los elementos especificados en este requisito.	Las vulnerabilidades de la seguridad del software a medida y personalizado son comúnmente explotadas por personas malintencionadas para obtener acceso a una red y comprometer los datos del tarjetahabiente. El código vulnerable es mucho más difícil y costoso de abordar una vez que se ha implementado o lanzado en entornos de producción. Exigir una revisión formal y la aprobación por parte de la gerencia antes de la publicación, contribuye a garantizar que el código se apruebe y se desarrolle de acuerdo con las políticas y procedimientos. **Buenas Prácticas** Los siguientes elementos deben considerarse para su inclusión en las revisiones de código: • Búsqueda de características no documentadas (herramientas de inserción, puertas traseras). • Confirmar que el software utiliza de forma segura las funciones de componentes externos (bibliotecas, marcos, API, etc.). Por ejemplo, si se utiliza una biblioteca de terceros que proporciona funciones criptográficas, verifique que esté integrada de forma segura. • Comprobación del uso correcto del registro para impedir que los datos confidenciales entren en los registros. • Análisis de estructuras de código inseguras que puedan contener vulnerabilidades potenciales relacionadas con ataques de software comunes identificados en los Requisitos 6.2.5. • Comprobación del comportamiento de la aplicación para detectar vulnerabilidades lógicas.
Objetivo del Enfoque Personalizado		
El software a medida y personalizado no puede explotarse a través de vulnerabilidades de codificación.		
Notas de Aplicabilidad		
Este requisito para las revisiones de código se aplica a todo el software a medida y personalizado (tanto interno como público), como parte del ciclo de vida de desarrollo del sistema. Las aplicaciones web públicas también están sujetas a controles adicionales para abordar las amenazas y vulnerabilidades continuas después de la implementación, como se define en el Requisito 6.4 PCI DSS. Las revisiones de código se pueden realizar mediante procesos manuales o automatizados, o una combinación de ambos.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
6.2.3.1 Si las revisiones manuales de código son realizadas para software hecho a medida y personalizado antes de ser liberado a producción, los cambios de código son: • Revisados por personas que no sean el autor del código original, y que conozcan las técnicas de revisión de código y las prácticas de codificación segura. • Revisados y aprobados por la dirección antes de su publicación.	**6.2.3.1.a** Si se realizan revisiones manuales del código para el software a medida y personalizado antes de su producción, examine los procedimientos documentados de desarrollo de software y entreviste al personal responsable para verificar que los procesos están definidos para que las revisiones manuales del código se realicen de acuerdo con todos los elementos especificados en este requisito.	El hecho de que el código sea revisado por alguien que no sea el autor original, que tenga experiencia en la revisión de código y que conozca las prácticas de codificación segura, minimiza la posibilidad de que el código que contenga errores de seguridad o lógicos que puedan afectar a la seguridad de los datos de los titulares de las tarjetas sea liberado en un entorno de producción. Exigir la aprobación de la gerencia de que el código ha sido revisado, limita la posibilidad de eludir el proceso.
Objetivo del Enfoque Personalizado	**6.2.3.1.b** Evalúe la evidencia de los cambios en el software a medida y personalizado y entreviste al personal para verificar que las revisiones manuales del código se realizaron de acuerdo con todos los elementos especificados en este requisito.	**Buenas Prácticas** Se ha comprobado que disponer de una metodología formal de revisión y de listas de verificación mejora la calidad del proceso de revisión del código. La revisión del código es un proceso agotador, y por esta razón, es más eficaz cuando los revisores sólo revisan pequeñas cantidades de código a la vez. Para mantener la eficacia de las revisiones de código, es beneficioso controlar la carga de trabajo general de los revisores y hacer que revisen aplicaciones con las que están familiarizados. Las revisiones de código se pueden realizar mediante procesos manuales o automatizados, o una combinación de ambos. Los titulares que dependen únicamente de la revisión manual del código deben asegurarse de que los revisores mantengan sus habilidades a través de la formación periódica a medida que se encuentran nuevas vulnerabilidades y se recomiendan nuevos métodos de codificación segura. *(continúa en la página siguiente)*
El proceso de revisión manual del código no se puede eludir y es eficaz para descubrir vulnerabilidades de seguridad.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Las revisiones manuales de código pueden ser llevadas a cabo por personal interno con conocimientos o por personal de terceros con conocimientos. Una persona a la que se le ha concedido formalmente la responsabilidad del control de la publicación y que no es ni el autor original del código ni el revisor del mismo cumple con los criterios de ser administrador.		**Información Adicional** Refiérase a la *Guía de Revisión del Código OWASP.*

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
6.2.4 Las técnicas de ingeniería de software u otros métodos están definidos y en uso para el software a medida y personalizado por el personal de desarrollo de software a fin de impedir o mitigar los ataques de software comunes y las vulnerabilidades relacionadas, incluyendo, pero no limitado a lo siguiente: • Ataques de inyección, incluyendo SQL, LDAP, XPath u otros fallos de flujo de tipo comando, parámetro, objeto, defecto o de inyección. • Ataques a datos y estructuras de datos, incluyendo intentos de manipulación de buffers, punteros, datos de entrada o datos compartidos. • Ataques al uso de criptografía, incluyendo intentos de explotar implementaciones criptográficas débiles, inseguras o inapropiadas, algoritmos, suites de cifrado o modos de operación. • Ataques a la lógica del negocio, incluyendo los intentos de abusar o eludir las características y funcionalidades de la aplicación a través de la manipulación de las APIs, los protocolos y canales de comunicación, la funcionalidad del lado del cliente, u otras funciones y recursos del sistema/aplicación. Esto incluye los scripts entre sitios (XSS) y la falsificación de petición entre sitios (CSRF). • Ataques a los mecanismos de control de acceso, incluidos los intentos de eludir o abusar de los mecanismos de identificación, autenticación o autorización, o los intentos de aprovechar las debilidades en la implementación de dichos mecanismos. *(continúa en la página siguiente)*	**6.2.4** Evalúe los procedimientos documentados y entreviste al personal responsable del desarrollo de software para verificar que las técnicas de ingeniería de software u otros métodos están definidos y en uso por los desarrolladores de software a medida y personalizado para impedir o mitigar todos los ataques de software comunes como se especifica en este requisito.	**Objetivo** Detectar o impedir los errores comunes que dan lugar a un código vulnerable lo más temprano posible dentro del proceso de desarrollo del software, reduce la probabilidad de que dichos errores lleguen a producción y den lugar a un riesgo de seguridad. Contar con técnicas y herramientas de ingeniería formal integradas en el proceso de desarrollo permitirá detectar estos errores en una fase temprana. Esta filosofía se llama a veces "desplazar la seguridad hacia la izquierda". **Buenas Prácticas** Tanto para el software a medida como para el personalizado, la entidad debe asegurarse de que el código se desarrolla centrándose en impedir o mitigar los ataques de software más comunes, incluyendo: • Intentos de explotar vulnerabilidades de codificación comunes (bugs). • Intentos de explotar los defectos de diseño del software. • Intentos de explotar fallos de implementación/configuración. • Ataques de enumeración: ataques automatizados que se explotan activamente en los pagos y abusan de los mecanismos de identificación, autenticación o autorización. Véase el artículo del blog *Perspectivas PCI "Cuidado con los ataques de comprobación de cuentas*." *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
• Ataques a través de cualquier vulnerabilidad de "alto riesgo" identificada en el proceso de identificación de vulnerabilidades, tal como se define en el Requisito 6.3.1. **Objetivo del Enfoque Personalizado** El software a medida y personalizado no puede explotarse a través de ataques comunes y sus vulnerabilidades relacionadas. **Notas de Aplicabilidad** Esto se aplica a todo el software desarrollado por o para la entidad para su propio uso. Esto incluye software tanto a medida como personalizado. Esto no aplica para el software de terceros.		Investigar y documentar las técnicas de ingeniería de software u otros métodos ayuda a definir cómo los desarrolladores de software impiden o mitigan varios ataques de software mediante características o contramedidas que incorporan al software. Esto podría incluir mecanismos de identificación/autenticación, control de acceso, rutinas de validación de entrada, etc. Los desarrolladores deben estar familiarizados con los diferentes tipos de vulnerabilidades y ataques potenciales y utilizar medidas para evitar posibles vectores de ataque cuando desarrollen el código. **Ejemplos** Las técnicas incluyen procesos y prácticas automatizadas que escanean el código en las primeras fases del ciclo de desarrollo cuando se comprueba el código para confirmar que las vulnerabilidades no están presentes.

Requisitos y Procedimientos de Prueba		Guía
6.3 Las vulnerabilidades de seguridad se identifican y son abordadas.		
Requisitos del Enfoque Definido **6.3.1** Las vulnerabilidades de seguridad se identifican y gestionan de la siguiente manera: • Las nuevas vulnerabilidades de seguridad se identifican utilizando fuentes reconocidas por la industria de información de vulnerabilidades de seguridad, incluyendo alertas de equipos internacionales y nacionales de respuesta a emergencias informáticas (CERTs). • A las vulnerabilidades se les asigna una clasificación de riesgo basada en las mejores prácticas de la industria y considerando su impacto potencial. • Las clasificaciones de riesgo identifican, como mínimo, todas las vulnerabilidades consideradas de alto riesgo o críticas para el entorno. • Se cubren las vulnerabilidades de los programas informáticos a medida y de terceros (por ejemplo, sistemas operativos y bases de datos). **Objetivo del Enfoque Personalizado** Las nuevas vulnerabilidades del sistema y del software que puedan afectar a la seguridad de los datos de cuentas o del CDE se monitorizan, se catalogan y se evalúan los riesgos.	**Procedimientos de Prueba del Enfoque Definido** **6.3.1.a** Evalúe las políticas y procedimientos para identificar y gestionar las vulnerabilidades de seguridad a fin de verificar que los procesos han sido definidos de acuerdo con todos los elementos especificados en este requisito. **6.3.1.b** Entreviste al personal responsable, examine la documentación y observe los procesos a fin de verificar que las vulnerabilidades de seguridad se identifican y gestionan de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** La clasificación de los riesgos (por ejemplo, como críticos, altos, medios o bajos) permite a las organizaciones identificar, priorizar y abordar los elementos de mayor riesgo más rápidamente y reducir la probabilidad de que se exploten las vulnerabilidades que presentan el mayor riesgo. **Buenas Prácticas** Los métodos para examinar las vulnerabilidades y asignar las clasificaciones de riesgo variarán en función del entorno y de la estrategia de evaluación de riesgos de una organización. Cuando una entidad está asignando sus clasificaciones de riesgo, debe considerar el uso de una metodología formal, objetiva y justificable que represente con precisión los riesgos de vulnerabilidades pertinentes a la organización, y que traduzca esas consideraciones en la asignación de un nivel de prioridad apropiado para su resolución. Los procesos de una organización para gestionar las vulnerabilidades deberían integrarse con otros procesos de gestión -por ejemplo, gestión de riesgos, gestión de cambios, gestión de parches, respuesta a incidentes, seguridad de las aplicaciones, así como una adecuada supervisión y registro de estos procesos. Esto ayudará a garantizar que todas las vulnerabilidades se identifiquen y sean abordadas apropiadamente. Los procesos deben respaldar las evaluaciones continuas de vulnerabilidades. Por ejemplo, una vulnerabilidad inicialmente identificada como de bajo riesgo podría convertirse en un riesgo mayor más adelante. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito no se consigue con los escaneos de vulnerabilidades realizados para los requisitos 11.3.1 y 11.3.2, ni es lo mismo. Este requisito se refiere a un proceso para monitorizar activamente las fuentes de la industria en materia de información de vulnerabilidades y para que la entidad determine la clasificación de riesgo que se asociará con cada vulnerabilidad.		Además, las vulnerabilidades, consideradas de forma individual como de riesgo bajo o medio, podrían representar colectivamente un riesgo alto o crítico si están presentes en el mismo sistema, o si se explotan en un sistema de bajo riesgo que podría dar lugar a un acceso al CDE. **Ejemplos** Algunas organizaciones que emiten alertas para asesorar a las entidades acerca de vulnerabilidades urgentes que requieran parches/actualizaciones inmediatas son los Equipos Nacionales de Preparación/Respuesta a Emergencias Informáticas (CERT) y los proveedores. Los criterios para clasificar las vulnerabilidades pueden incluir el nivel de criticidad de una vulnerabilidad identificada en una alerta del Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST) o de un CERT, la consideración de la puntuación CVSS, la clasificación del proveedor y/o el tipo de sistemas afectados. **Información Adicional** Las fuentes confiables de información sobre vulnerabilidades son los sitios web de los proveedores, los grupos de noticias del sector, las listas de correo, etc. Si el software se desarrolla internamente, el equipo de desarrollo interno también debe considerar las fuentes de información sobre nuevas vulnerabilidades que puedan afectar las aplicaciones desarrolladas internamente. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
		Otros métodos para garantizar que se identifiquen nuevas vulnerabilidades incluyen soluciones que reconocen y pasan alertas automáticas al detectar un comportamiento inusual. Los procesos deben tomar en consideración las vulnerabilidades ampliamente publicadas, al igual que los ataques de "día cero" que apuntan a vulnerabilidades previamente desconocidas. Para software a medida y personalizado, la organización puede obtener información sobre bibliotecas, marcos, compiladores, lenguajes de programación, etc. de fuentes públicas confiables (por ejemplo, recursos especiales y recursos de desarrolladores de componentes). La organización también puede analizar de forma independiente componentes de terceros e identificar vulnerabilidades. Para controlar el software desarrollado internamente, la organización puede recibir dicha información de fuentes externas. La organización puede considerar el uso de un programa de "recompensa por errores" en el que publica información (por ejemplo, en su sitio web) para que terceros puedan comunicarse con la organización con información sobre vulnerabilidades. Las fuentes externas pueden incluir investigadores independientes o empresas que informan a la organización sobre las vulnerabilidades identificadas y pueden incluir fuentes como el Sistema de Medidas de Evaluación de Vulnerabilidades (CVSS) o la Metodología de Calificación de Riesgo OWASP.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Identificar y enumerar todo el software personalizado y a medida de la entidad y cualquier software de terceros que se incorpore al software personalizado y a medida de la entidad, permite gestionar vulnerabilidades y parches. Las vulnerabilidades en componentes de terceros (incluidas bibliotecas, API, etc.) integradas en el software de una entidad también hacen que esas aplicaciones sean vulnerables a los ataques. A fin de garantizar la seguridad del software es esencial saber qué componentes de terceros se utilizan en el software de la entidad y monitorizar la disponibilidad de parches de seguridad para abordar las vulnerabilidades conocidas. **Buenas Prácticas** El inventario de una entidad debe cubrir todos los componentes y dependencias del software de pago, incluidas las plataformas o entornos de ejecución compatibles, bibliotecas de terceros, servicios y otras funcionalidades requeridas. Hay muchos tipos diferentes de soluciones que pueden ayudar con la administración de inventarios de software, como herramientas de análisis de composición del software, herramientas de descubrimiento de aplicaciones y administración de dispositivos móviles.
6.3.2 A fin de facilitar la gestión de vulnerabilidades y parches se mantiene un inventario del software a medida y personalizado y de los componentes del software de terceros incorporados en el software a medida y personalizado.	**6.3.2.a** Evalúe la documentación y entreviste al personal para verificar que se mantenga un inventario del software a medida y personalizado y de los componentes del software de terceros incorporados a ese software, y que el inventario se utilice para identificar y abordar las vulnerabilidades.	
Objetivo del Enfoque Personalizado	**6.3.2.b** Evalúe la documentación del software, incluido el software a medida y personalizado que integra componentes del software de terceros, y compárelo con el inventario para verificar que incluya el software a medida y personalizado y los componentes del software de terceros.	
Las vulnerabilidades conocidas en componentes del software de terceros no pueden explotarse en el software a medida y personalizado.		
Notas de Aplicabilidad		
Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
6.3.3 Todos los componentes del sistema están protegidos contra vulnerabilidades conocidas mediante la instalación de parches/actualizaciones de seguridad aplicables de la siguiente manera: • Los parches/actualizaciones críticas o de alta seguridad (identificados de acuerdo con el proceso de clasificación de riesgos del Requisito 6.3.1) se instalan dentro del período de un mes de su emisión. • Todos los demás parches/actualizaciones de seguridad aplicables se instalan dentro de un período de tiempo apropiado según lo determine la entidad (por ejemplo, dentro de los tres meses posteriores al lanzamiento).	**6.3.3.a** Evalúe las políticas y procedimientos para verificar que los procesos estén definidos para abordar vulnerabilidades mediante la instalación de parches/actualizaciones de seguridad aplicables de acuerdo con todos los elementos especificados en este requisito. **6.3.3.b** Evalúe los componentes del sistema y el software relacionado y comparar la lista de parches/actualizaciones de seguridad instaladas con la información de actualización/parche de seguridad más reciente a fin de verificar que las vulnerabilidades se aborden de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Constantemente se descubren nuevas vulnerabilidades que pueden permitir ataques contra sistemas que anteriormente se consideraban seguros. Si los parches/actualizaciones de seguridad más recientes no se implementan en los sistemas críticos lo antes posible, actores malintencionados pueden utilizar esas vulnerabilidades para atacar o deshabilitar un sistema u obtener acceso a datos confidenciales. **Buenas Prácticas** Dar prioridad a los parches/actualizaciones de seguridad para la infraestructura crítica garantiza que los sistemas y dispositivos altamente prioritarios estén protegidos contra vulnerabilidades tan pronto como sea posible después de que se publique un parche. La cadencia de parcheo de una entidad debe tener en cuenta cualquier reevaluación de vulnerabilidades y cambios subsecuentes en el nivel de criticidad de una vulnerabilidad según el Requisito 6.3.1. Por ejemplo, una vulnerabilidad inicialmente identificada como de bajo riesgo podría convertirse en un riesgo alto más adelante. Además, las vulnerabilidades, consideradas de forma individual como de riesgo bajo o medio, podrían representar colectivamente un riesgo alto o crítico si están presentes en el mismo sistema, o si se explotan en un sistema de bajo riesgo que podría dar lugar a un acceso al CDE.
Objetivo del Enfoque Personalizado		
Los componentes del sistema no pueden verse comprometidos mediante la explotación de una vulnerabilidad conocida.		

Requisitos y Procedimientos de Prueba		Guía
6.4 Las aplicaciones web públicas están protegidas contra ataques.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Las aplicaciones web de cara al público son aquellas que están disponibles para el público (no sólo para uso interno). Dichas aplicaciones son los objetivos principales de los atacantes, y las aplicaciones web mal codificadas proporcionan una vía fácil para que los atacantes accedan a datos y sistemas confidenciales. **Buenas Prácticas** Las herramientas o métodos de evaluación de la seguridad de las vulnerabilidades, sean manuales o automatizados, revisan y/o ponen a prueba la aplicación en busca de vulnerabilidades. Las herramientas de evaluación más comunes incluyen escáneres web especializados que realizan un análisis automático de la protección de las aplicaciones web. Cuando se utilicen soluciones técnicas automatizadas, es importante incluir procesos que faciliten una respuesta oportuna a las alertas generadas por las soluciones, a fin de poder mitigar cualquier ataque que haya sido detectado. **Ejemplos** F*irewalls* de aplicaciones web (WAF) instalado delante de las aplicaciones web de cara al público para comprobar todo el tráfico es un ejemplo de solución técnica automatizada que detecta e impide los ataques basados en la web (por ejemplo, los ataques incluidos en el Requisito 6.2.4). Los WAF filtran y bloquean el tráfico no esencial en la capa de aplicación. Un WAF correctamente configurado ayuda a impedir los ataques en la capa de aplicación de las aplicaciones que están codificadas o configuradas de forma indebida. *(continúa en la página siguiente)*
6.4.1 Para las aplicaciones web de cara al público, las nuevas amenazas y vulnerabilidades se abordan de forma continua y están protegidas contra los ataques conocidos de la siguiente manera: • Revisión de las aplicaciones web de cara al público mediante herramientas o métodos de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, sean manuales o automatizadas, como sigue: – Al menos una vez cada 12 meses y después de cambios significativos. – Por una entidad especializada en seguridad de aplicaciones. – Incluyendo, como mínimo, todos los ataques de software comunes descritos en el Requisito 6.2.4. – Todas las vulnerabilidades se clasifican de acuerdo con el Requisito 6.3.1. – Se corrigen todas las vulnerabilidades. – La aplicación se vuelve a examinar después de las correcciones. **O** • Instalación de soluciones técnicas automatizadas que detecten e impidan continuamente los ataques basados en la web de la siguiente manera: – Instaladas frente a las aplicaciones web de cara al público para detectar e impedir los ataques basados en la web. – Generando registros de auditoría. *(continúa en la página siguiente)*	**6.4.1** Para las aplicaciones web de cara al público, asegúrese de que cada uno de los métodos requeridos está ubicado en su lugar como sigue: • Si se utilizan herramientas o métodos manuales o automatizados de evaluación de la seguridad de las vulnerabilidades, examine los procesos documentados, entreviste al personal y examine los registros de las evaluaciones de la seguridad de las aplicaciones para verificar que las aplicaciones web de cara al público se revisan de acuerdo con todos los elementos de este requisito específicos a la herramienta/método. **O** • Si se instala una solución técnica automatizada que detecte e impida continuamente los ataques basados en la web, examine los ajustes de configuración del sistema y los registros de auditoría, y entreviste al personal responsable para verificar que la solución técnica automatizada está instalada de acuerdo con todos los elementos de este requisito específicos de la solución o soluciones.	

Requisitos y Procedimientos de Prueba		Guía
– Configurados ya sea para bloquear los ataques basados en la web o para generar una alerta que se investigue inmediatamente.		Otro ejemplo de solución técnica automatizada son las tecnologías de Autoprotección de Aplicaciones en Tiempo de Ejecución (RASP). Cuando se implementan correctamente, las soluciones RASP pueden detectar y bloquear comportamientos anómalos del software durante su ejecución. Mientras que los WAF típicamente monitorean el perímetro de la aplicación, las soluciones RASP vigilan y bloquean el comportamiento dentro de la aplicación.
Objetivo del Enfoque Personalizado		
Las aplicaciones web de cara al público están protegidas contra ataques maliciosos.		
Notas de Aplicabilidad		
Esta evaluación no es la misma que los escaneos de vulnerabilidad realizados para los Requisitos 11.3.1 y 11.3.2. Este requisito será sustituido por el requisito 6.4.2 después del 31 de marzo de 2025, cuando entre en vigor el requisito 6.4.2.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
6.4.2 Para aplicaciones web de cara al público se implementa una solución técnica automatizada que detecta e impide continuamente ataques basados en la web, con al menos lo siguiente: • Se instala frente a aplicaciones web de cara al público y está configurado para detectar e impedir ataques basados en la web. • Funcionando activamente y actualizándose según corresponda. • Generando registros de auditoría. • Configurados ya sea para bloquear los ataques basados en la web o para generar una alerta que se investigue inmediatamente.	**6.4.2** Para las aplicaciones web de cara al público, examine los ajustes de configuración del sistema y los registros de auditoría, y entreviste al personal responsable para verificar que se haya implementado una solución técnica automatizada que detecte e impida los ataques basados en la web de acuerdo con todos los elementos especificados en este requisito.	Las aplicaciones web de cara al público son los principales objetivos de los atacantes, y las aplicaciones web mal codificadas proporcionan una vía fácil para que los atacantes accedan a datos y sistemas confidenciales. **Buenas Prácticas** Cuando se utilicen soluciones técnicas automatizadas, es importante incluir procesos que faciliten una respuesta oportuna a las alertas generadas por las soluciones, a fin de poder mitigar cualquier ataque que haya sido detectado. Estas soluciones también pueden utilizarse para automatizar la mitigación, por ejemplo, los controles de limitación de velocidad que pueden aplicarse para mitigar los ataques de fuerza bruta y los ataques de enumeración. **Ejemplos** F*irewalls* de aplicaciones web (WAF), que puede ubicarse en las instalaciones o estar basado en la nube, instalado frente a las aplicaciones web de cara al público para comprobar todo el tráfico, es un ejemplo de solución técnica automatizada que detecta e impide los ataques basados en la web (por ejemplo, los ataques descritos en el Requisito 6.2.4). Los WAF filtran y bloquean el tráfico no esencial en la capa de aplicación. Un WAF correctamente configurado ayuda a impedir los ataques en la capa de aplicación de las aplicaciones que están codificadas o configuradas de forma indebida.
Objetivo del Enfoque Personalizado		
Las aplicaciones web de cara al público están protegidas en tiempo real contra ataques maliciosos.		
Notas de Aplicabilidad		
Este nuevo requisito reemplazará al Requisito 6.4.1 una vez que termine su fecha de vigencia. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
6.4.3 Todos los scripts de las páginas de pago que se cargan y ejecutan en el navegador del consumidor se gestionan de la siguiente manera: • Se implementa un método para confirmar que cada script está autorizado. • Se implementa un método para asegurar la integridad de cada script. • Se mantiene un inventario de todos los scripts con una justificación por escrito que explique su necesidad.	**6.4.3.a** Evalúe las políticas y los procedimientos para verificar que los procesos están definidos para gestionar todos los scripts de las páginas de pago que se cargan y ejecutan en el navegador del consumidor, de acuerdo con todos los elementos especificados en este requisito.	Los scripts cargados y ejecutados en la página de pago pueden tener su funcionalidad alterada sin el conocimiento de la entidad y también pueden tener la funcionalidad de cargar scripts externos adicionales (por ejemplo, publicidad y seguimiento, sistemas de administración de etiquetas). Los atacantes potenciales pueden utilizar estos scripts aparentemente inofensivos para cargar scripts maliciosos que pueden leer y filtrar los datos del titular de la tarjeta desde el navegador del consumidor. Asegurarse de que se entienda que la funcionalidad de todos estos scripts es necesaria para el funcionamiento de la página de pago minimiza el número de scripts que podrían ser falsificados. Asegurarse de que los scripts han sido explícitamente autorizados reduce la probabilidad de que se agreguen secuencias de comandos innecesarias a la página de pago sin la aprobación de la administración correspondiente. El uso de técnicas para evitar la falsificación del script minimizará la probabilidad de que este se modifique para realizar una acción no autorizada, como robar los datos del titular de la tarjeta de la página de pago. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado	**6.4.3.b** Entreviste al personal responsable y examine los registros de inventario y las configuraciones del sistema para verificar que todos los scripts de páginas de pago que se cargan y ejecutan en el navegador del consumidor se gestionan de acuerdo con todos los elementos especificados en este requisito.	
El código no autorizado no puede estar en la página de pago tal y como se presenta en el navegador del consumidor.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito se aplica a todos los scripts cargados desde el entorno de la entidad y a los scripts cargados desde terceras y cuartas partes. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		**Buenas Prácticas** Los scripts pueden ser autorizados por procesos manuales o automatizados (por ejemplo, flujo de trabajo). Cuando la página de pago se cargue en un marco en línea (IFRAME), restringiendo la ubicación desde la que se puede cargar la página de pago, el uso de la Política de Seguridad de Contenido (CSP) de la página principal puede ayudar a evitar que se sustituya la página de pago por contenido no autorizado. **Definiciones** "Necesario", en el marco de este requisito, significa que la revisión de la entidad de cada script justifica y confirma por qué es necesario para que la página de pago pueda desarrollar sus funciones al aceptar una transacción de pago. **Ejemplos** Todos los scripts pueden reforzarse mediante distintos mecanismos incluyendo, pero sin limitarse: • Integridad de sub-recursos (SRI), lo que permite al navegador del consumidor validar que un script no ha sido manipulado. • Un CSP, que limita las ubicaciones desde las cuales el navegador del consumidor puede cargar un script y transmitirle datos de cuentas. • Sistemas propios de gestión de scripts o etiquetas, que pueden impedir la ejecución de scripts maliciosos.

Requisitos y Procedimientos de Prueba		Guía
6.5 Los cambios en todos los componentes del sistema se gestionan de forma segura.		
Requisitos del Enfoque Definido **6.5.1** Los cambios en todos los componentes del sistema en el entorno de producción se realizan de acuerdo con los procedimientos establecidos que incluyen: • Motivo y descripción del cambio. • Documentación del impacto a la seguridad. • Aprobación documentada del cambio por las partes autorizadas. • Pruebas para verificar que el cambio no afecta negativamente la seguridad del sistema. • En el caso de los cambios de software a la medida y personalizados, todas las actualizaciones se comprueban para determinar que cumplen con el requisito 6.2.4 antes de ser instalados para producción. • Procedimientos para hacer frente a los fallos y volver a un estado seguro. **Objetivo del Enfoque Personalizado** Todos los cambios se rastrean, se autorizan y se evalúan en cuanto a su impacto y seguridad, y los cambios se gestionan para evitar efectos no deseados en la seguridad de los componentes del sistema.	**Procedimientos de Prueba del Enfoque Definido** **6.5.1.a** Evalúe los procedimientos documentados de control de cambios para verificar que los procedimientos para los cambios en todos los componentes del sistema del entorno de producción están definidos, a fin de incluir todos los elementos especificados en este requisito. **6.5.1.b** Evalúe los cambios recientes a los componentes del sistema y rastrear esos cambios hasta la documentación de control de cambios relacionada. Para cada cambio evaluado, verifique que el cambio se aplica de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Los procedimientos de gestión de cambios deben aplicarse a todos los cambios -incluyendo la adición, eliminación o modificación de cualquier componente del sistema- en el entorno de producción. Es importante documentar la razón de un cambio y la descripción del mismo, de manera que las partes relevantes entiendan y estén de acuerdo en que el cambio es necesario. Asimismo, el documentar los impactos del cambio, permite a todas las partes afectadas planificar adecuadamente cualquier cambio en el proceso. **Buenas Prácticas** La aprobación de las partes autorizadas confirma que el cambio es legítimo y aprobado por la organización. Los cambios deben ser aprobados por personas con la autoridad y los conocimientos adecuados para comprender el impacto de ese cambio. La realización de pruebas exhaustivas por parte de la entidad confirma que la seguridad del entorno no se vea afectada por la aplicación de cambios; y que todos los controles de seguridad existentes se mantienen o son sustituidos por controles de seguridad iguales o más fuertes después del cambio. Las pruebas específicas que deben realizarse variarán en función del tipo de cambio y del componente o componentes del sistema que se vean afectados. Para cada cambio, es importante tener procedimientos documentados que aborden cualquier fallo y proporcionen instrucciones sobre cómo volver a un estado seguro en caso de que el cambio falle o afecte negativamente la seguridad de una aplicación o sistema. Estos procedimientos permitirán restaurar la aplicación o el sistema a su estado seguro anterior.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Tener procesos para analizar cambios significativos ayuda a garantizar que todos los controles apropiados PCI DSS se apliquen a cualquier sistema o red agregado o cambiado dentro del entorno y alcance, y que se sigan cumpliendo los requisitos de PCI DSS para proteger ese entorno. **Buenas Prácticas** La incorporación de esta validación en los procesos de gestión de cambios ayuda a garantizar que los inventarios de dispositivos y los estándares de configuración se mantengan actualizados y que se apliquen controles de seguridad donde sea necesario. **Ejemplos** Los requisitos aplicables PCI DSS que podrían verse afectados incluyen, entre otros: • Los diagramas de flujo de datos y redes se actualizan para reflejar los cambios. • Los sistemas se configuran según los estándares de configuración, con todas las contraseñas predeterminadas cambiadas y los servicios innecesarios deshabilitados. • Los sistemas están protegidos con los controles necesarios, por ejemplo, monitoreo de la integridad de los archivos (FIM), antimalware, parches y registro de auditoría. • Los datos confidenciales de autenticación no se almacenan, y todo el almacenamiento de datos de cuentas está documentado e incorporado en la política y los procedimientos de retención de datos. • Los nuevos sistemas se incluyen en el proceso de análisis de vulnerabilidades trimestral. *(continúa en la página siguiente)*
6.5.2 Al completar un cambio significativo, se confirma que todos los requisitos de PCI DSS están vigentes en todos los sistemas y redes nuevas o modificadas, y la documentación se actualiza según corresponda.	**6.5.2** Evalúe la documentación en busca de cambios significativos, entreviste al personal y observe los sistemas/redes afectados para verificar que la entidad confirmó que los requisitos de PCI DSS estaban vigentes en todos los sistemas y redes nuevas o modificadas, y que la documentación fue actualizada según corresponda.	
Objetivo del Enfoque Personalizado		
Todos los componentes del sistema se verifican después de un cambio significativo para que cumplan con los requisitos de PCI DSS aplicables.		

<table>
<tr><th colspan="2">Requisitos y Procedimientos de Prueba</th><th>Guía</th></tr>
<tr><td colspan="2">Notas de Aplicabilidad

Estos cambios significativos también deben capturarse y reflejarse en la actividad de confirmación del alcance PCI DSS anual de la entidad, según el Requisito 12.5.2.</td><td>• Los sistemas son escaneos en busca de vulnerabilidades internas y externas después de cambios significativos según los Requisitos 11.3.1.3 y 11.3.2.1.</td></tr>
<tr><td>Requisitos del Enfoque Definido</td><td>Procedimientos de Prueba del Enfoque Definido</td><td rowspan="4">Objetivo
Debido al constante estado de cambio de los entornos de pre-producción, a menudo son menos seguros que el entorno de producción.
Buenas Prácticas
Las organizaciones deben comprender claramente qué entornos son entornos de prueba o entornos de desarrollo y cómo estos entornos interactúan a nivel de redes y aplicaciones.
Definiciones
Los entornos de preproducción incluyen desarrollo, pruebas, pruebas de aceptación del usuario (UAT), etc. Incluso cuando la infraestructura de producción se utiliza para facilitar las pruebas o el desarrollo, los entornos de producción deben separarse (lógica o físicamente) de las funciones de pre-producción, de modo que las vulnerabilidades introducidas como resultado de las actividades de pre-producción no afecten negativamente a los sistemas de producción.</td></tr>
<tr><td rowspan="3">6.5.3 Los entornos de preproducción se separan de los entornos de producción y la separación se aplica con controles de acceso.</td><td>6.5.3.a Evalúe las políticas y los procedimientos para verificar que los procesos estén definidos para separar el entorno de pre-producción del entorno de producción a través de controles de acceso que refuerzan la separación.</td></tr>
<tr><td>6.5.3.b Evalúe la documentación de la red y las configuraciones de los controles de seguridad de la red a fin de asegurarse de que el entorno de pre-producción esté separado de los entornos de producción.</td></tr>
<tr><td>6.5.3.c Evalúe la configuración del control de acceso para confirmar que los controles de acceso estén en su lugar para aplicar la separación entre los entornos de pre-producción y de producción.</td></tr>
<tr><td colspan="2">Objetivo del Enfoque Personalizado

Los entornos de pre-producción no pueden generar riesgos y vulnerabilidades en los entornos de producción.</td></tr>
</table>

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
6.5.4 Los roles y las funciones se separan entre los entornos de producción y pre-producción para asignar responsabilidades de manera tal que sólo se desplieguen los cambios revisados y aprobados.	**6.5.4.a** Evalúe las políticas y procedimientos para verificar que los procesos están definidos para separar los roles y las funciones para asignar responsabilidad de manera tal que sólo se desplieguen los cambios revisados y aprobados. **6.5.4.b** Observe los procesos y entreviste al personal para verificar que los controles implementados separan los roles y las funciones y asignan las responsabilidades de manera tal que sólo se desplieguen los cambios revisados y aprobados.	El objetivo de separar roles y funciones entre los entornos de producción y preproducción es reducir la cantidad de personal con acceso al entorno de producción y datos de cuentas y, por lo tanto, minimizar el riesgo de acceso no autorizado, no intencional o inadecuado a los datos. y componentes del sistema y ayudar a garantizar que el acceso esté limitado a aquellas personas con una necesidad de negocio de dicho acceso. La intención de este control es separar las actividades críticas para supervisarlas y revisarlas a fin de detectar errores y minimizar las posibilidades de fraude o robo (ya que dos personas tendrían que confabularse para ocultar una actividad). La separación de roles y funciones, también denominada separación o segregación de funciones, es un concepto de control interno clave para proteger los activos de una entidad.
Objetivo del Enfoque Personalizado		
Las funciones y la responsabilidad que diferencian las actividades de pre-producción y producción se definen y gestionan para minimizar el riesgo de acciones no autorizadas, involuntarias o inapropiadas.		
Notas de Aplicabilidad		
En entornos con personal limitado donde los individuos desempeñan múltiples roles o funciones, este mismo objetivo puede lograrse con controles de procedimiento adicionales que asignen responsabilidades. Por ejemplo, un desarrollador puede ser también un administrador que utiliza una cuenta de nivel administrador con privilegios especiales en el entorno de desarrollo y, para su función de desarrollador, utiliza una cuenta separada con acceso de nivel de usuario al entorno de producción.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
6.5.5 Los datos PAN activos no se utilizan en entornos de pre-producción, excepto cuando esos entornos están incluidos en el CDE y protegidos de acuerdo con todos los requisitos de PCI DSS aplicables.	**6.5.5.a** Evalúe las políticas y procedimientos para verificar que los procesos estén definidos para no usar datos PAN activos en entornos de pre-producción, excepto cuando esos entornos están incluidos en el CDE y protegidos de acuerdo con todos los requisitos de PCI DSS aplicables.	**Objetivo** El uso de datos PAN activos fuera de los CDE protegidos proporciona a individuos maliciosos la oportunidad de obtener acceso no autorizado a los datos de los titulares de tarjetas. **Buenas Prácticas** Las entidades pueden minimizar su almacenamiento de datos PAN activos almacenándolos sólo en pre-producción cuando sea estrictamente necesario para un propósito de prueba específico y definido y eliminando de forma segura esos datos después de su uso. Si una entidad requiere datos PAN específicamente diseñados para fines de prueba, éstos pueden obtenerse de los adquirientes. **Definiciones** Los datos PAN activos se refieren a datos PAN válidos (no datos PAN de prueba) que tienen el potencial de utilizarse para realizar transacciones de pago. Además, cuando las tarjetas de pago vencen, los mismos datos PAN a menudo se reutilizan con una fecha de caducidad diferente. Todos los datos PAN deben verificarse para determinar que no son aptos para realizar transacciones de pago antes de que se excluyan del alcance PCI DSS. Es responsabilidad de la entidad confirmar que los datos PAN no estén activos.
	6.5.5.b Observe los procedimientos de prueba y entreviste al personal para verificar que se han establecido procedimientos para garantizar que no se utilicen PAN vivos en entornos de preproducción, excepto cuando dichos entornos se encuentren en un CDE y estén protegidos de acuerdo con todos los requisitos de PCI DSS aplicables.	
Objetivo del Enfoque Personalizado	**6.5.5.c** Evalúe los datos de prueba de preproducción para verificar que las PAN activos no se utilicen en entornos de preproducción, excepto cuando esos entornos estén en un CDE y estén protegidos de acuerdo con todos los requisitos de PCI DSS aplicables.	
Los datos PAN activos no pueden estar presentes en entornos de pre-producción fuera del CDE.		

<table>
<tr><th colspan="2">Requisitos y Procedimientos de Prueba</th><th>Guía</th></tr>
<tr><td>Requisitos del Enfoque Definido</td><td>Procedimientos de Prueba del Enfoque Definido</td><td rowspan="4">Objetivo
Estos datos pueden revelar información sobre el funcionamiento de una aplicación o sistema y son un blanco fácil de explotar para que personas no autorizadas obtengan acceso a los sistemas. La posesión de dicha información podría facilitar el compromiso del sistema y los datos de cuentas relacionados.</td></tr>
<tr><td rowspan="2">6.5.6 Los datos de prueba y las cuentas de pruebas se eliminan de los componentes del sistema antes de que el sistema entre en producción.</td><td>6.5.6.a Evalúe las políticas y los procedimientos para verificar que los procesos estén definidos para la eliminación de datos de prueba y cuentas de prueba de los componentes del sistema, antes de que el sistema entre en producción.</td></tr>
<tr><td>6.5.6.b Observe los procesos de prueba tanto para el software estándar como para las aplicaciones internas, y entreviste al personal para verificar que los datos de prueba y las cuentas de prueba se eliminen antes de que un sistema entre en producción.</td></tr>
<tr><td>Objetivo del Enfoque Personalizado

Los datos y cuentas de prueba no pueden existir en entornos de producción.</td><td>6.5.6.c Observe los datos y las cuentas del software estándar y las aplicaciones internas instaladas o actualizadas recientemente para verificar que no haya datos de prueba ni cuentas de prueba en los sistemas en producción.</td></tr>
</table>

Implementar Medidas Sólidas de Control de Acceso

Requisito 7: Restringir el Acceso a los Componentes del Sistema y a los Datos de Tarjetahabientes Según la Necesidad de Conocimiento de la Empresa

Secciones	
7.1	Se definen y comprenden los procesos y mecanismos para restringir el acceso a los componentes del sistema y a los datos del titular de la tarjeta según la necesidad de negocio de conocerlos.
7.2	El acceso a los componentes y datos del sistema se define y asigna adecuadamente.
7.3	El acceso a los componentes y datos del sistema se gestiona a través de un sistema de control de acceso.

Descripción

Las personas no autorizadas pueden obtener acceso a datos o sistemas críticos debido a reglas y definiciones de control de acceso ineficientes. Para garantizar que sólo el personal autorizado pueda tener acceso a los datos críticos, se deben implementar sistemas y procesos para limitar el acceso según la necesidad de conocer y de acuerdo con las responsabilidades de cada puesto de trabajo.

El "acceso" o los "derechos de acceso" se crean mediante reglas que brindan a los usuarios acceso a los sistemas, aplicaciones y datos, mientras que los "privilegios" permiten al usuario realizar una acción o función específica en relación con ese sistema, aplicación o base de datos. Por ejemplo, un usuario puede tener derechos de acceso a datos específicos, pero son sus privilegios los que determinan si sólo puede leer esos datos, o si también puede cambiar o eliminar los datos.

La "necesidad de conocer" se refiere a facilitar el acceso solamente a la menor cantidad posible de datos necesarios para realizar un trabajo.

Los "privilegios mínimos" se refieren a proporcionar únicamente el nivel mínimo de privilegios necesarios para realizar un trabajo.

Estos requisitos aplican a las cuentas de usuario y al acceso para empleados, contratistas, consultores y proveedores internos y externos y otros terceros (por ejemplo, para brindar servicios de apoyo de mantenimiento). Ciertos requisitos también se aplican a las cuentas del sistema y de la aplicación utilizadas por la entidad (también llamadas "cuentas de servicio").

Estos requisitos no aplican para los consumidores (titulares de tarjetas).

Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
7.1 Se definen y comprenden los procesos y mecanismos para restringir el acceso a los componentes del sistema y los datos del titular de la tarjeta según la necesidad de negocio.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** El Requisito 7.1.1 trata sobre la gestión y el mantenimiento eficiente de las diversas políticas y procedimientos especificados en el Requisito 7. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 7, es igualmente importante garantizar que se documenten, se mantengan y se difundan adecuadamente. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocios. Por esta razón, considere actualizar estos documentos lo más pronto posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.
7.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 7 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.	**7.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 7 son administrados de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado		
Las expectativas, los controles y la vigilancia en el cumplimiento con las actividades dentro del Requisito 7 están definidos y cumplidos por el personal afectado. Todas las actividades de apoyo son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que las actividades críticas no se desarrollen. **Buenas Prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
7.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 7 están documentadas, asignadas y son comprendidos.	**7.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y responsabilidades para realizar las actividades del Requisito 7 estén documentadas y asignadas.	
	7.1.2.b Entreviste al personal responsable de desarrollar las actividades del Requisito 7 para verificar que los roles y responsabilidades se asignen según sean documentadas y entendidas.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 7. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
7.2 El acceso a los componentes y datos del sistema se define y asigna adecuadamente.		
Requisitos del Enfoque Definido **7.2.1** Se define un modelo de control de acceso que incluye la autorización de acceso como sigue: • Acceso apropiado según el tipo de negocios de la entidad y las necesidades de acceso. • Acceso a los componentes del sistema y a los recursos de datos basados en la clasificación y las funciones del trabajo de los usuarios. • Los privilegios mínimos requeridos (por ejemplo, usuario, administrador) para realizar una función laboral. **Objetivo del Enfoque Personalizado** Se establecen los requisitos de acceso de acuerdo con las funciones laborales siguiendo los principios de privilegio mínimo y necesidad de conocer.	**Procedimientos de Prueba del Enfoque Definido** **7.2.1.a** Evalúe las políticas y procedimientos documentados y entreviste al personal para verificar que el modelo de control de acceso esté definido con todos los elementos especificados en este requisito. **7.2.1.b** Evalúe la configuración del modelo de control de acceso y verificar que las necesidades de acceso estén definidas de manera apropiada en concordancia con todos los elementos especificados en este requisito.	**Objetivo** La definición de un modelo de control de acceso que sea apropiado para la tecnología de la entidad y la filosofía de control de acceso respalda una forma consistente y uniforme de asignar el acceso y reduce la posibilidad de errores como la concesión de derechos excesivos. **Buenas Prácticas** Un factor a considerar al definir las necesidades de acceso es el principio de separación de funciones. El objetivo de este principio es impedir el fraude y el uso inapropiado o robo de los recursos. Por ejemplo, 1) dividir las funciones críticas de misión de las funciones de soporte del sistema de información entre diferentes individuos y/o funciones, 2) establecer funciones de manera que las actividades de soporte del sistema de información sean realizadas por diferentes funciones/individuos (por ejemplo, administración del sistema, programación, configuración gestión, control de calidad y pruebas, y seguridad de la red) y 3) garantizar que el personal de seguridad que administra las funciones de control de acceso no administre también las funciones de auditoría. En entornos donde una persona realiza funciones múltiples, como operaciones de administración y seguridad, se pueden asignar tareas para que ninguna persona tenga el control de un proceso de un extremo a otro sin un punto de control independiente. Por ejemplo, la responsabilidad de la configuración y la responsabilidad de aprobar los cambios podrían asignarse a diferentes personas. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
		Definiciones Los elementos clave de un modelo de control de acceso incluyen: • Recursos a proteger (los sistemas/dispositivos/datos a los que se necesita acceder), • Funciones del puesto de trabajo que necesitan acceso al recurso (por ejemplo, administrador del sistema, personal del centro de llamadas, empleado de la tienda), y • Qué actividades debe realizar cada función laboral (por ejemplo, lectura/escritura o consulta). Una vez que se definen las funciones laborales, los recursos y las actividades por funciones laborales, se puede otorgar acceso a las personas en ese sentido. **Ejemplos** Los modelos de control de acceso que las entidades pueden considerar incluyen el control de acceso basado en roles (RBAC) y el control de acceso basado en atributos (ABAC). El modelo de control de acceso utilizado por una entidad determinada depende de sus necesidades de negocios y necesidades de acceso.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
7.2.2 El acceso se asigna a los usuarios, incluidos los privilegiados, en función de: • La clasificación y función del trabajo. • Los privilegios mínimos necesarios para realizar las responsabilidades del trabajo.	**7.2.2.a** Evalúe las políticas y procedimientos para verificar que cubren la asignación de acceso a los usuarios de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** La aplicación de privilegios mínimos ayuda a evitar que los usuarios que no tengan suficiente conocimiento de la aplicación cambien de forma incorrecta o accidental su configuración o alteren su configuración de seguridad. Aplicar los privilegios mínimos también ayuda a minimizar el alcance de los daños si una persona no autorizada obtiene acceso a la ID de un usuario. **Buenas Prácticas** Los derechos de acceso se conceden a un usuario mediante la asignación de una o varias funciones. La evaluación se asigna dependiendo de las funciones específicas del usuario y con el alcance mínimo requerido para el trabajo. Al asignar un acceso privilegiado, es importante asignar a los individuos solo los privilegios que requieran para hacer su trabajo (los "privilegios mínimos"). Por ejemplo, al administrador de la base de datos o al administrador de las copias de apoyo, no se le deben asignar los mismos privilegios que al administrador general de los sistemas. Una vez definidas las necesidades de las funciones de los usuarios (según el requisito 7.2.1 PCI DSS), es fácil conceder a los individuos el acceso de acuerdo con la clasificación de su trabajo y su función utilizando los roles ya creados. Las entidades pueden considerar el uso de la Gestión de Accesos Privilegiados (PAM), que es un método para conceder acceso a cuentas privilegiadas sólo cuando esos privilegios son necesarios, revocando inmediatamente ese acceso una vez que ya no son necesarios.
	7.2.2.b Evalúe las configuraciones de acceso de los usuarios, incluidos los usuarios con privilegios, y entreviste al personal de gestión responsable de verificar que los privilegios asignados se ajustan a todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado El acceso a los sistemas y a los datos se limita únicamente al acceso necesario para realizar las funciones del trabajo, tal y como se define en los roles de acceso correspondientes.	**7.2.2.c** Entreviste al personal responsable de asignar el acceso para verificar que el acceso de los usuarios con privilegios se asigna de acuerdo con todos los elementos especificados en este requisito.	

<table>
<tr><th colspan="2">Requisitos y Procedimientos de Prueba</th><th>Guía</th></tr>
<tr><td>Requisitos del Enfoque Definido</td><td>Procedimientos de Prueba del Enfoque Definido</td><td rowspan="4">Objetivo
La aprobación documentada (por ejemplo, por escrito o electrónicamente) garantiza que las personas con acceso y privilegios son conocidas y están autorizadas por la dirección, y que su acceso es necesario para su función laboral.</td></tr>
<tr><td>7.2.3 Los privilegios requeridos son aprobados por el personal autorizado.</td><td>7.2.3.a Evalúe las políticas y procedimientos para verificar que definen los procesos para la aprobación de todos los privilegios por parte del personal autorizado.</td></tr>
<tr><td rowspan="2">Objetivo del Enfoque Personalizado

No se pueden conceder privilegios de acceso a los usuarios sin la autorización apropiada y documentada.</td><td>7.2.3.b Evalúe las identificaciones de los usuarios y los privilegios asignados, y compararlos con las aprobaciones documentadas para asegurarse de que:
• Existe una aprobación documentada para los privilegios asignados.
• La aprobación fue realizada por personal autorizado.
• Los privilegios especificados coinciden con las funciones asignadas a la persona.</td></tr>
</table>

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
7.2.4 Todas las cuentas de usuario y los privilegios de acceso relacionados, incluyendo las cuentas de terceros/proveedores, se revisan de la siguiente manera: • Al menos una vez cada seis meses. • Para asegurarse de que las cuentas de usuario y el acceso sigan siendo apropiados según la función del trabajo. • Se aborda cualquier acceso inadecuado. • La gerencia reconoce que el acceso sigue siendo apropiado.	**7.2.4.a** Evalúe las políticas y los procedimientos para verificar que definen los procesos de revisión de todas las cuentas de usuario y los privilegios de acceso relacionados, incluidas las cuentas de terceros/proveedores, de acuerdo con todos los elementos especificados en este requisito.	La revisión periódica de los derechos de acceso ayuda a detectar los derechos de acceso excesivos que quedan después de que cambian las responsabilidades laborales de los usuarios, las funciones del sistema u otras modificaciones. Si los derechos de acceso de un usuario son excesivos y no se revocan a su debido tiempo, pueden ser utilizados por usuarios malintencionados para acceder sin autorización. Esta revisión ofrece otra oportunidad para garantizar que se han eliminado las cuentas de todos los usuarios dados de baja (si es que faltaba alguna en el momento de la baja), así como también para asegurarse de que se haya dado de baja a cualquier tercero que ya no necesite acceso.
Objetivo del Enfoque Personalizado	**7.2.4.b** Entreviste al personal responsable y examine los resultados documentados de las revisiones periódicas de las cuentas de usuarios para verificar que todos los resultados estén de acuerdo con todos los elementos especificados en este requisito.	**Buenas Prácticas** Cuando un usuario se traslada a una nueva función o a un nuevo departamento, normalmente los privilegios y el acceso asociados a su antigua función ya no son necesarios. El acceso continuado a privilegios o funciones que ya no son necesarios pueden generar un riesgo de mal uso o errores. Por lo tanto, cuando las responsabilidades cambian, los procesos que revalidan el acceso ayudan a garantizar que el acceso del usuario es apropiado para sus nuevas responsabilidades. Las entidades pueden considerar implementar un proceso regular y repetible para desarrollar revisiones de los derechos de acceso, y asignar "propietarios de datos" que sean responsables de gestionar y supervisar el acceso a los datos relacionados con su función de trabajo y que también garanticen que el acceso del usuario sigue siendo vigente y es apropiado. *(continúa en la página siguiente)*
Las asignaciones de privilegios de cuenta son verificadas periódicamente por la gerencia como correctas y se corrigen las inconformidades.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito se aplica a todas las cuentas de usuario y privilegios de acceso relacionados incluyendo las que utiliza el personal y terceros/proveedores, y las cuentas utilizadas para acceder a servicios de terceros en la nube. Consulte los Requisitos 7.2.5 y 7.2.5.1 y 8.6.1 a 8.6.3 para conocer los controles de aplicaciones y cuentas del sistema. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		Por ejemplo, un gerente directo podría revisar el acceso de los miembros de su equipo de trabajo mensualmente, mientras que el gerente general revisa el acceso de sus grupos de trabajo trimestralmente, y ambos realizan las actualizaciones de acceso que sean necesarias. La intención de estas mejores prácticas es apoyar y facilitar la realización de las revisiones al menos una vez cada 6 meses.
Requisitos del Enfoque Definido **7.2.5** Todas las aplicaciones y cuentas del sistema y los privilegios de acceso relacionados se asignan y administran de la siguiente manera: • Basado en los privilegios mínimos necesarios para la operatividad del sistema o aplicación. • El acceso está limitado a los sistemas, aplicaciones o procesos que específicamente requieren su uso. **Objetivo del Enfoque Personalizado** Los derechos de acceso otorgados a las cuentas del sistema y de aplicaciones se limitan únicamente al acceso necesario para la operación de esa aplicación o sistema.	**Procedimientos de Prueba del Enfoque Definido** **7.2.5.a** Evalúe las políticas y los procedimientos para verificar que definen los procesos de administración y asignación de las cuentas de usuario y aplicaciones, y los privilegios de acceso relacionados, de acuerdo con todos los elementos especificados en este requisito. **7.2.5.b** Evalúe los privilegios relacionados con las cuentas del sistema y de aplicaciones y entreviste al personal responsable para verificar que las cuentas del sistema y de aplicaciones, y los privilegios de acceso relacionados, se asignen y administren de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Es importante establecer el nivel de acceso apropiado para la aplicación o las cuentas del sistema. Si dichas cuentas se ven comprometidas, usuarios malintencionados recibirán el mismo nivel de acceso que el otorgado a la aplicación o al sistema. Por lo tanto, es importante asegurarse de que se otorgue un acceso limitado a las cuentas del sistema y de la aplicación de la misma manera que a las cuentas de los usuarios. **Buenas Prácticas** Es posible que las entidades consideren establecer una base de referencia al configurar las cuentas de aplicaciones y sistemas, incluyendo las siguientes, según corresponda a la organización: *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		• Asegurarse de que la cuenta no sea miembro de un grupo privilegiado como administradores de dominio, administradores locales o root. • Restringir en qué computadoras se puede usar la cuenta. • Restricción de las horas de uso. • Eliminar cualquier configuración adicional como acceso VPN y acceso remoto.
Requisitos del Enfoque Definido **7.2.5.1** Todo el acceso de aplicaciones y cuentas del sistema y los privilegios de acceso relacionados se revisan de la siguiente manera: • Periódicamente, (a una frecuencia definida en el análisis de riesgos específico de la entidad, el cual se desarrolla de acuerdo a todos los elementos especificados en el Requisito 12.3.1.). • El acceso a la aplicación/sistema sigue siendo apropiado para la función que se está realizando. • Se aborda cualquier acceso inadecuado. • La gerencia reconoce que el acceso sigue siendo apropiado. **Objetivo del Enfoque Personalizado** Las asignaciones de privilegios de aplicaciones y cuentas de sistemas son verificadas periódicamente por la gerencia como correctas, y se corrigen las inconformidades.	**Procedimientos de Prueba del Enfoque Definido** **7.2.5.1.a** Evalúe las políticas y los procedimientos para verificar que definen los procesos de revisión de todas las cuentas de aplicaciones y sistemas, y privilegios de acceso relacionados, de acuerdo con todos los elementos especificados en este requisito. **7.2.5.1.b** Evalúe el análisis de riesgo específico de la entidad para conocer la frecuencia de las evaluaciones periódicas de las cuentas de sistemas y aplicaciones y los privilegios de acceso relacionados para verificar que el análisis de riesgo se realizó de acuerdo con todos los elementos especificados en el Requisito 12. 3. 1. **7.2.5.1.c** Entreviste al personal responsable y examine los resultados documentados de las revisiones periódicas de las cuentas de usuarios y de aplicaciones y los privilegios relacionados a fin de verificar que las revisiones se realizan de acuerdo con lo especificados en este requisito.	**Objetivo** La revisión periódica de los derechos de acceso ayuda a detectar derechos de acceso excesivos que permanecen después de un cambio de funciones del sistema o se producen otras modificaciones en la aplicación o el sistema. Si los derechos de usuario excesivos no se revocan cuando ya no se necesitan, pueden ser utilizados por usuarios malintencionados para acceder sin autorización.

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		
Requisitos del Enfoque Definido **7.2.6** Todo acceso por parte de los usuarios a las bases de datos de los titulares de la tarjeta está restringido de la siguiente manera: • A través de aplicaciones u otros métodos programáticos, con acceso y acciones permitidas basadas en las funciones y privilegios mínimos del usuario. • Solo los administradores autorizados pueden acceder directamente o consultar las bases de datos de CHD almacenados. **Objetivo del Enfoque Personalizado** Se prohíbe el acceso directo a consultas sin filtrar (ad hoc) a las bases de datos de titulares de tarjetas, a menos que lo realice un administrador autorizado. **Notas de Aplicabilidad** Este requisito se aplica a los controles para el acceso de los usuarios a las bases de datos almacenados de titulares de tarjetas. Consulte los Requisitos 7.2.5 y 7.2.5.1 y 8.6.1 a 8.6.3 para conocer los controles para aplicaciones y cuentas del sistema.	**Procedimientos de Prueba del Enfoque Definido** **7.2.6.a** Evalúe las políticas y los procedimientos y entreviste al personal para verificar que los procesos estén definidos para otorgar acceso de usuario a la consulta de datos almacenados de titulares de tarjetas, de acuerdo con todos los elementos especificados en este requisito. **7.2.6.b** Evalúe la configuración para consultar las bases de datos de los titulares de tarjetas a fin de verificar que cumplen con todos los elementos especificados en este requerimiento.	**Objetivo** El uso indebido del acceso a consultas de bases de datos de titulares de tarjetas es una causa común de filtración de datos. Limitar dicho acceso a los administradores reduce el riesgo de que usuarios no autorizados abusen de dicho acceso. **Definiciones** "Métodos programáticos" significa otorgar acceso a través de medios tales como procedimientos almacenados en la base de datos, lo que permiten a los usuarios realizar acciones controladas a los datos en una tabla, en lugar de a través del acceso directo y sin filtrar el acceso a la base de datos por parte de los usuarios finales (excepto los administradores responsables), quienes necesitan acceso directo a la base de datos para sus funciones administrativas). **Buenas Prácticas** Las acciones típicas del usuario incluyen mover, copiar y eliminar datos. También considere el alcance del privilegio necesario al otorgar el acceso. Por ejemplo, se puede otorgar acceso a puntos específicos como elementos de datos, archivos, tablas, índices, vistas y rutinas almacenadas. Al otorgar acceso a la base de datos de los titulares de tarjetas se debe seguir el mismo proceso que para todos los demás accesos otorgados; es decir el procedimiento debe basarse en las funciones, y asignar a cada usuario sólo los privilegios que sean necesarios para realizar sus funciones laborales.

Requisitos y Procedimientos de Prueba		Guía
7.3 El acceso a los componentes y datos del sistema se gestiona a través de un sistema de control de acceso.		
Requisitos del Enfoque Definido **7.3.1** Existen sistemas de control de acceso que restringen el acceso según la necesidad del usuario y cubre todos los componentes del sistema. **Objetivo del Enfoque Personalizado** Los derechos y privilegios de acceso se gestionan mediante mecanismos destinados para tal fin.	**Procedimientos de Prueba del Enfoque Definido** **7.3.1** Evalúe la documentación del proveedor y la configuración del sistema para verificar que el acceso se administre, para cada componente del sistema, a través de controles de acceso que restringen el acceso según la necesidad del usuario y cubren todos los componentes del sistema.	**Objetivo** Sin un mecanismo para restringir el acceso basado en la necesidad de conocimiento del usuario, el usuario puede erróneamente obtener acceso a los datos de titulares de la tarjeta. Los sistemas de control de acceso automatizan el proceso de restringir el acceso y asignar privilegios.
Requisitos del Enfoque Definido **7.3.2** Los sistemas de control de acceso están configurados para aplicar los permisos asignados a individuos, aplicaciones, y sistemas basados en la clasificación y función del trabajo. **Objetivo del Enfoque Personalizado** Los derechos y privilegios individuales de acceso a cuentas de sistemas, aplicaciones y datos sólo se heredan a través de la pertenencia a un grupo.	**Procedimientos de Prueba del Enfoque Definido** **7.3.2** Evalúe la documentación del proveedor y la configuración del sistema para verificar que los sistemas de control de acceso están configurados para aplicar los permisos asignados a individuos, aplicaciones y sistemas basados en la clasificación y función del trabajo.	**Objetivo** Restringir el acceso privilegiado con un sistema de control de acceso reduce la posibilidad de errores en la asignación de los permisos a individuos, aplicaciones y sistemas.

<table>
<tr><th colspan="2">Requisitos y Procedimientos de Prueba</th><th>Guía</th></tr>
<tr><td>Requisitos del Enfoque Definido</td><td>Procedimientos de Prueba del Enfoque Definido</td><td rowspan="3">Objetivo
Una configuración predeterminada de "denegar todo" garantiza que no se conceda acceso a nadie a menos que se establezca una regla específica que conceda dicho acceso.
Buenas Prácticas
Es importante comprobar la configuración predeterminada de los sistemas de control de acceso, ya que algunos están configurados por defecto para "permitir todo", otorgando así el acceso a menos que/hasta que se escriba una regla para negarlo específicamente.</td></tr>
<tr><td>7.3.3 El sistema de control de acceso está configurado para "denegar todo" predeterminadamente.</td><td>7.3.3 Evalúe la documentación del proveedor y la configuración del sistema para verificar que el sistema de control de acceso está configurado predeterminadamente para "denegar todo".</td></tr>
<tr><td>Objetivo del Enfoque Personalizado</td><td></td></tr>
<tr><td>Los derechos y privilegios de acceso están prohibidos a menos que se permitan expresamente.</td><td></td><td></td></tr>
</table>

Requisito 8: Identificar a los Usuarios y Autenticar el Acceso a los Componentes del Sistema

Secciones	
8.1	Los procesos y mecanismos para identificar a los usuarios y autenticar el acceso a los componentes del sistema están definidos y son comprendidos.
8.2	La identificación de usuarios y las cuentas relacionadas para usuarios y administradores se gestionan estrictamente durante el ciclo de vida de una cuenta.
8.3	Se establece y gestiona una autenticación fuerte para usuarios y administradores.
8.4	Se implementa la autenticación de múltiples factores (MFA) para proteger el acceso al CDE.
8.5	Los sistemas de autenticación de múltiples factores (MFA) están configurados para evitar su uso indebido.
8.6	El uso de cuentas de aplicaciones y sistemas y los factores de autenticación asociados se gestionan estrictamente.

Descripción

Dos principios fundamentales de la identificación y de la autenticación de usuarios son: 1) establecer la identidad de un individuo o proceso en un sistema informático, y 2) probar o verificar que el usuario asociado a la identidad es quien dice ser.

La identificación de un individuo o proceso en un sistema informático se lleva a cabo asociando una identidad con una persona o proceso a través de un identificador, como un ID de usuario, sistema o aplicación. Estos identificadores (también denominados "cuentas") establecen fundamentalmente la identidad de un individuo o proceso asignando un ID único a cada persona o proceso para distinguir un usuario o proceso de otro. Cuando cada usuario o proceso puede ser identificado de forma única, se garantiza la responsabilidad de las acciones realizadas por esa identidad. Cuando dicha responsabilidad existe, las acciones realizadas pueden ser rastreadas hasta usuarios y procesos conocidos y autorizados.

El elemento utilizado para probar o verificar la identidad se conoce como factor de autenticación. Los factores de autenticación son: 1) algo que uno sabe, como una contraseña o frase de paso, 2) algo que uno tiene, como un dispositivo token o una tarjeta inteligente, o 3) algo que uno es, como un elemento biométrico.

El ID y el factor de autenticación se consideran conjuntamente credenciales de autenticación y se utilizan para obtener acceso a los derechos y privilegios asociados con las cuentas de un usuario, aplicación, sistema o servicio.

(continúa en la página siguiente)

Estos requisitos de identidad y autenticación se basan en principios de seguridad aceptados por la industria y en las mejores prácticas para apoyar el ecosistema de pagos. *La Publicación Especial 800-63 del NIST, Directrices de Identidad Digital, proporciona información adicional sobre los marcos aceptables para la identidad digital y factores de autenticación.* Es importante tener en cuenta que las *Directrices de Identidad Digital del NIST* están destinadas a las Agencias Federales de los Estados Unidos y deben ser examinadas en su totalidad. Se espera que muchos de los conceptos y enfoques definidos en estas directrices funcionen entre sí y no como parámetros independientes.

***Nota**: A menos que se indique lo contrario en el requisito, estos requisitos se aplican a **todas las cuentas de todos los componentes del sistema,** a menos que se indique específicamente en un requisito individual, que incluya, entre otros:*

- *Cuentas de punto de venta*
- *Cuentas con capacidades administrativas*
- *Cuentas de sistema y de aplicación*
- *Todas las cuentas que se utilizan para ver o acceder a los datos de titulares de tarjetas o para acceder a sistemas con datos de titulares de tarjetas.*

Esto incluye cuentas utilizadas por empleados, contratistas, consultores, proveedores internos y externos y otros terceros (por ejemplo, para brindar servicios de soporte o mantenimiento).

Ciertos requisitos no están destinados a aplicarse a cuentas de usuario que tienen acceso a un solo número de tarjeta a la vez para facilitar una sola transacción (como las identificaciones utilizadas por los cajeros en terminales de punto de venta). Cuando los elementos no aplican, se indican directamente dentro del requisito específico.

Estos requisitos no aplican para los consumidores (titulares de tarjetas).

Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
8.1 Los procesos y mecanismos para identificar a los usuarios y autenticar el acceso a los componentes del sistema están definidos y son comprendidos.		
Requisitos del Enfoque Definido **8.1.1** Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 8 están: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la vigilancia para el cumplimiento con las actividades del Requisito 8 están definidos y son seguidos por el personal afectado. Todas las actividades de soporte son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.	**Procedimientos de Prueba del Enfoque Definido** **8.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 8 son administrados de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** El Requisito 8.1.1 trata sobre la gestión y el mantenimiento eficiente de las diversas políticas y procedimientos descritos en el Requisito 8. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 8, es igualmente importante garantizar que se documenten, se mantengan y se difundan adecuadamente. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocios. Por esta razón, considere actualizar estos documentos lo antes posible después de que haya ocurrido un cambio y no únicamente en ciclos periódicos. **Definiciones** Las políticas de seguridad definen los objetivos y principios de la seguridad en la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 8 están documentados, asignados y son comprendidos.	**8.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y responsabilidades para realizar las actividades del Requisito 8 estén documentadas y asignadas.	Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que, por lo tanto, las actividades críticas no se realicen.
	8.1.2.b Entreviste al personal responsable de desarrollar las actividades del Requisito 8 para verificar que los roles y responsabilidades son asignados según la documentación y son comprendidos.	**Buenas Prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de la comunicación de los roles y responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de los roles y responsabilidades que les han sido asignados.
Objetivo del Enfoque Personalizado		**Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 8. El personal es responsable del continuo y correcto funcionamiento de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
8.2 La identificación de usuarios y las cuentas relacionadas para usuarios y administradores se gestionan estrictamente durante el ciclo de vida de una cuenta.		
Requisitos del Enfoque Definido **8.2.1** A todos los usuarios se les asigna un ID único antes de permitirles el acceso a los componentes del sistema o a los datos del titular de la tarjeta. **Objetivo del Enfoque Personalizado** Todas las acciones de todos los usuarios son atribuibles a un individuo. **Notas de Aplicabilidad** Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los *IDs* utilizados por los cajeros en los terminales de punto de venta).	**Procedimientos de Prueba del Enfoque Definido** **8.2.1.a** Entreviste al personal responsable para verificar que a todos los usuarios se les asigna un ID único para acceder a los componentes del sistema y a los datos del titular de la tarjeta. **8.2.1.b** Evalúe los registros de auditoría y otras pruebas para verificar que el acceso a los componentes del sistema y a los datos de los titulares de tarjetas puede identificarse de forma exclusiva y asociarse a las personas.	**Objetivo** La capacidad de rastrear las acciones realizadas en un sistema informático por un individuo, establece la responsabilidad y la trazabilidad, y es fundamental para establecer controles de acceso eficientes. Al garantizar que cada usuario se identifique de forma única, en lugar de utilizar un ID para varios empleados, la organización puede mantener la responsabilidad individual de las acciones, y un registro de auditoría eficiente por empleado. Además, esto ayudará en la resolución y contención de problemas cuando se dé un mal uso o una intención maliciosa.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.2.2 Las cuentas grupales, compartidas o genéricas, u otras credenciales de autenticación compartidas sólo se usan cuando es necesario, de manera excepcional, y se administran de la siguiente manera: • Se impide el uso de la cuenta a menos que se requiera por una circunstancia excepcional. • Su uso está limitado al tiempo necesario para la circunstancia excepcional. • La justificación de negocio para su uso está documentada. • Su uso está explícitamente aprobado por la dirección. • La identidad del usuario individual se confirma antes de que se conceda el acceso a una cuenta. • Cada acción realizada es atribuible a un usuario individual.	**8.2.2.a** Evalúe las listas de cuentas de usuario en los componentes del sistema y la documentación aplicable para verificar que las credenciales de autenticación compartidas solo se utilicen cuando sea necesario, de manera excepcional, y se administren de acuerdo con todos los elementos especificados en este requisito.	Las cuentas de grupo, compartidas o genéricas (o predeterminadas) suelen entregarse con los programas informáticos o los sistemas operativos, por ejemplo, como root o con privilegios asociados a una función específica, como la de administrador. Si varios usuarios comparten las mismas credenciales de autenticación (por ejemplo, cuenta de usuario y contraseña), resulta imposible rastrear el acceso y las actividades del sistema a un individuo. A su vez, esto impide que una entidad asigne responsabilidad por, o tenga un registro efectivo de, las acciones de un individuo, ya que una determinada acción podría haber sido realizada por cualquier persona del grupo con conocimiento del ID de usuario y los factores de autenticación asociados. La capacidad de asociar personas a las acciones realizadas con una cuenta es esencial para proporcionar responsabilidad individual y trazabilidad con respecto a quién realizó una acción, qué acción se realizó y cuándo ocurrió esa acción.
Objetivo del Enfoque Personalizado	**8.2.2.b** Evalúe las políticas y los procedimientos de autenticación para verificar que los procesos para las credenciales de autenticación compartidas estén definidos, de modo que solo se utilicen cuando sea necesario, de forma excepcional, y se gestionen de acuerdo con todos los elementos especificados en este requisito.	**Buenas Prácticas** Si se utilizan cuentas compartidas por cualquier motivo, se deben establecer controles de gestión sólidos para mantener la responsabilidad individual y la trazabilidad.
Todas las acciones realizadas por usuarios con ID genéricos, del sistema o compartidos, son atribuibles a una persona individual.	**8.2.2.c** Entreviste a los administradores del sistema para verificar que las credenciales de autenticación compartidas sólo se usan cuando es necesario, de manera excepcional, y se administran de acuerdo con todos los elementos especificados en este requisito.	*(continúa en la página siguiente)*
Notas de Aplicabilidad		
Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los IDs utilizados por los cajeros en los terminales de punto de venta).		

Requisitos y Procedimientos de Prueba		Guía
		Ejemplos Existen herramientas y técnicas que pueden facilitar tanto la administración como la seguridad de este tipo de cuentas y confirmar la identidad del usuario individual antes de que se otorgue el acceso a una cuenta. Las entidades pueden considerar gestores de contraseñas u otros controles administrados por el sistema, como el comando *sudo.* Un ejemplo de una circunstancia excepcional es cuando todos los demás métodos de autenticación han fallado y se necesita una cuenta compartida para uso de emergencia o "romper el cristal" para un acceso de administrador.
Requisitos del Enfoque Definido **8.2.3** ***Requisito adicional solo para proveedores de servicios:*** Los proveedores de servicios con acceso remoto a las instalaciones del cliente deben utilizar factores de autenticación únicos para las instalaciones de cada cliente. **Objetivo del Enfoque Personalizado** Las credenciales de un proveedor de servicios utilizadas para un cliente no se pueden utilizar para ningún otro cliente. *(continúa en la página siguiente)*	**Procedimientos de Prueba del Enfoque Definido** **8.2.3** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe las políticas y los procedimientos de autenticación y entreviste al personal para verificar que los proveedores de servicios con acceso remoto a las instalaciones del cliente utilicen factores de autenticación únicos para el acceso remoto a las instalaciones de cada cliente.	**Objetivo** Los proveedores de servicios con acceso remoto a las instalaciones del cliente suelen utilizar este acceso para respaldar los sistemas POS POI o para proporcionar otros servicios remotos. Si un proveedor de servicios utiliza los mismos factores de autenticación para acceder a varios clientes, todos los clientes del proveedor de servicios pueden verse fácilmente comprometidos si un atacante compromete ese factor. Los delincuentes saben esto y se dirigen deliberadamente a los proveedores de servicios en busca de un factor de autenticación compartido que les brinde acceso remoto a varios comercios a través de ese único factor. **Ejemplos** Tecnologías como los mecanismos multifactoriales que proporcionan una credencial única para cada conexión (como contraseñas de un solo uso) también podrían cumplir con la intención de este requisito.

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios. Este requisito no aplica a los proveedores de servicios que acceden a sus propios entornos de servicios compartidos, donde se alojan múltiples entornos de clientes. Si los empleados del proveedor de servicios utilizan factores de autenticación compartidos para acceder de forma remota a las instalaciones del cliente, estos factores deben ser únicos para cada cliente y deben administrarse de acuerdo con el Requisito 8.2.2.		
Requisitos del Enfoque Definido **8.2.4** La creación, eliminación y modificación de *IDs* de usuario, factores de autenticación y otros objetos de identificación se gestiona de la siguiente manera: • Autorizado con la aprobación correspondiente. • Implementado solo con los privilegios especificados en la aprobación documentada. **Objetivo del Enfoque Personalizado** Los eventos del ciclo de vida de los *IDs* de usuario y los factores de autenticación no pueden ocurrir sin la autorización adecuada.	**Procedimientos de Prueba del Enfoque Definido** **8.2.4** Evalúe las autorizaciones documentadas en varias fases del ciclo de vida de la cuenta (creaciones, modificaciones y eliminaciones) y examine la configuración del sistema para verificar que la actividad se haya administrado de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Es imperativo que el ciclo de vida de una ID de usuario (creaciones, eliminaciones y modificaciones) sea controlado, de manera que sólo las cuentas autorizadas puedan realizar funciones, que las acciones sean auditables y que los privilegios se limiten solamente a lo requerido. Los atacantes a menudo ponen en peligro una cuenta existente y luego escalan los privilegios de esa cuenta para realizar actos no autorizados, o pueden crear nuevas identificaciones para continuar su actividad en segundo plano. Es fundamental detectar y responder cuando se crean o modifican cuentas de usuario fuera del

<table>
<tr><th colspan="2">Requisitos y Procedimientos de Prueba</th><th>Guía</th></tr>
<tr><td>Notas de Aplicabilidad

Este requisito se aplica a todas las cuentas de usuario, incluyendo los empleados, contratistas, consultores, trabajadores temporales y proveedores externos.</td><td></td><td>proceso normal de cambio o sin la correspondiente autorización.</td></tr>
<tr><td>Requisitos del Enfoque Definido

8.2.5 El acceso para los usuarios que cesan se revoca inmediatamente.</td><td>Procedimientos de Prueba del Enfoque Definido

8.2.5.a Evalúe las fuentes de información para los usuarios cesantes y revise las listas de acceso de los usuarios actuales, tanto para el acceso local como para el remoto, a fin de verificar que las identificaciones de los usuarios cesantes se hayan desactivado o eliminado de las listas de acceso.

8.2.5.b Entreviste al personal responsable para verificar que todos los factores de autenticación físicos – tales como tarjetas inteligentes, tokens, etc., se hayan devuelto o desactivado para los usuarios deshabilitados.</td><td rowspan="2">Objetivo

Si un empleado interno o un tercero/proveedor dejaron la empresa y aún tiene acceso a la red a través de su cuenta de usuario, podría ocurrir un acceso innecesario o malicioso a los datos de titulares de tarjetas, ya sea por parte del ex-empleado o por parte de usuarios malintencionados valiéndose de la cuenta antigua y/o no utilizada.</td></tr>
<tr><td>Objetivo del Enfoque Personalizado

No se pueden utilizar las cuentas de los usuarios cesantes.</td><td></td></tr>
</table>

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **8.2.6** Las cuentas de usuario inactivas se eliminan o inhabilitan dentro de los 90 días de inactividad. **Objetivo del Enfoque Personalizado** No se pueden utilizar cuentas de usuario inactivas.	**Procedimientos de Prueba del Enfoque Definido** **8.2.6** Evalúe las cuentas de usuario y la información del último inicio de sesión, y entreviste al personal para verificar que las cuentas de usuario inactivas se eliminen o deshabiliten dentro de los 90 días de inactividad.	**Objetivo** Las cuentas que no se utilizan regularmente suelen ser objetivos de ataques, ya que es menos probable que se noten cambios, como, por ejemplo, un cambio de contraseña. De esta forma, estas cuentas pueden explotarse más fácilmente y usarse para acceder a los datos del titular de la tarjeta. **Buenas Prácticas** Cuando se pueda anticipar razonablemente que una cuenta no se utilizará durante un período prolongado de tiempo, como una excedencia prolongada, la cuenta debe desactivarse tan pronto como comience la baja, en lugar de esperar 90 días.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Permitir que terceros tengan acceso las 24 horas del día, los 7 días de la semana a los sistemas y redes de una entidad con el propósito de brindar soporte, aumenta las posibilidades de acceso no autorizado. Este acceso podría llevar a que un usuario no autorizado en el entorno del tercero, o a un individuo malintencionado, utilizar este punto de entrada externo siempre disponible en la red de una entidad. Cuando terceros necesitan acceso las 24 horas del día, los 7 días de la semana, debe documentarse, justificarse, monitorizarse y vincularse a razones específicas del servicio. **Buenas Prácticas** Habilitar el acceso sólo durante los períodos de tiempo necesarios y deshabilitarlo tan pronto como ya no sea necesario, ayuda a evitar el uso indebido de estas conexiones. Además, considere asignar a terceros una fecha de inicio y finalización de acceso, de acuerdo con su contrato de servicio. Monitorizar el acceso de terceros ayuda a garantizar que los terceros accedan solamente a los sistemas necesarios y sólo durante los períodos de tiempo aprobados. Se debe realizar un seguimiento y resolver cualquier actividad inusual que utilice cuentas de terceros.
8.2.7 Las cuentas utilizadas por terceros para acceder, respaldar o mantener componentes del sistema a través de acceso remoto se administran de la siguiente manera: • Son habilitadas solamente durante el período de tiempo necesario y son deshabilitadas cuando no están en uso. • Su uso es monitorizado para detectar cualquier actividad inesperada.	**8.2.7** Entreviste al personal, examine la documentación para administrar las cuentas y examine las evidencias necesarias para verificar que las cuentas utilizadas por terceros para el acceso remoto se administran de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado		
El acceso remoto de terceros no se puede utilizar, excepto donde esté específicamente autorizado y el uso sea supervisado por la gerencia.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **8.2.8** Si una sesión de usuario ha estado inactiva durante más de 15 minutos, se requiere que el usuario vuelva a autenticarse para reactivar el terminal o la sesión. **Objetivo del Enfoque Personalizado** Una sesión de usuario no puede ser utilizada a excepción del propio usuario autorizado. **Notas de Aplicabilidad** Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los *IDs* utilizados por los cajeros en los terminales de punto de venta). Este requisito no pretende impedir que se realicen actividades legítimas mientras la consola/PC está desatendida.	**Procedimientos de Prueba del Enfoque Definido** **8.2.8** Evalúe los ajustes de configuración del sistema para verificar que las características de tiempo máximo de inactividad del sistema/sesión para las sesiones de usuario se han establecido en 15 minutos o menos.	**Objetivo** Cuando los usuarios se ausentan de una máquina abierta con acceso a los componentes del sistema o a los datos de titulares de tarjetas, existe el riesgo de que la máquina sea utilizada por otros en ausencia del usuario, lo que resultaría en un acceso no autorizado a la cuenta y/o su uso indebido. **Buenas Prácticas** La re-autenticación se puede aplicar a nivel del sistema para proteger todas las sesiones que se ejecutan en esa máquina o a nivel de la aplicación. Las entidades también pueden considerar la posibilidad de organizar controles en sucesión para restringir aún más el acceso de una sesión desatendida a medida que pasa el tiempo. Por ejemplo, el protector de pantalla puede activarse después de 15 minutos y cerrar la sesión del usuario después de una hora. Sin embargo, los controles de tiempo máximo de inactividad deben equilibrar el riesgo de acceso y exposición con el impacto en el usuario y el propósito del acceso. Si un usuario necesita ejecutar un programa desde un equipo desatendido, el usuario puede iniciar sesión en el equipo para iniciar el programa y luego "bloquear" el equipo para que nadie más pueda usar el inicio de sesión del usuario mientras está desatendido. **Ejemplos** Una forma de cumplir este requisito es configurar un salvapantallas automático que se inicie cada vez que la consola esté inactiva durante 15 minutos y que requiera que el usuario conectado introduzca su contraseña para desbloquear la pantalla.

Requisitos y Procedimientos de Prueba		Guía
8.3 Se establece y gestiona una autenticación fuerte para usuarios y administradores.		
Requisitos del Enfoque Definido **8.3.1** Todo acceso por parte de los usuarios y administradores a componentes del sistema se autentifica utilizando al menos uno de los siguientes factores de autenticación: • Algo que uno sabe, como una contraseña o frase de paso. • Algo que uno tiene, como un dispositivo *token* o una tarjeta inteligente. • Algo que uno es, como un elemento biométrico. **Objetivo del Enfoque Personalizado** Sólo se puede acceder a una cuenta mediante la combinación de la identidad del usuario y de un factor de autenticación. **Notas de Aplicabilidad** Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los *IDs* utilizados por los cajeros en los terminales de punto de venta). Este requisito no sustituye a los requisitos de autenticación de múltiples factores (MFA), sino que se aplica a los sistemas incluidos en el ámbito de aplicación que no están sujetos a los requisitos de los MFA. El certificado digital es una opción válida para "algo que se tiene" si es único para un usuario concreto.	**Procedimientos de Prueba del Enfoque Definido** **8.3.1.a** Evalúe la documentación que describa el factor o factores de autenticación utilizados para verificar que el acceso del usuario a los componentes del sistema se autentifica mediante al menos un factor de autenticación especificado en este requisito. **8.3.1.b** Para cada tipo de factor de autenticación utilizado con cada tipo de componente del sistema, observe el proceso de autenticación para verificar que la autenticación funciona de forma coherente con el factor o factores de autenticación documentados.	**Objetivo** Cuando es utilizado además del I*D* único, el factor de autenticación ayuda a proteger dichos *IDs* de ser comprometidos, ya que el atacante necesita tener el *ID* único y poner en riesgo los factores de autenticación asociados. **Buenas Prácticas** Un enfoque común que individuos maliciosos emplean para comprometer un sistema es explotar factores de autenticación débiles o inexistentes (como, por ejemplo, contraseñas/frases de paso). Exigir factores de autenticación fuertes ayuda a protegerse contra este tipo de ataque. **Información Adicional** Consulte *fidoalliance.org* para obtener más información sobre el uso de *tokens,* tarjetas inteligentes o biometría como factores de autenticación.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.3.2 Se utiliza criptografía sólida para que todos los factores de autenticación sean ilegibles durante la transmisión y el almacenamiento en todos los componentes del sistema.	**8.3.2.a** Evalúe documentación de fabricante así como los ajustes de configuración del sistema para verificar que los factores de autenticación se vuelven ilegibles mediante criptografía sólida durante la transmisión y el almacenamiento.	Se sabe que los dispositivos de red y las aplicaciones transmiten factores de autenticación legibles y desencriptados (como contraseñas y frases de paso) a través de la red y/o almacenan estos valores sin cifrar. Como resultado, individuos malintencionados pueden interceptar fácilmente esta información durante la transmisión utilizando un "*sniffer",* o acceder directamente a los factores de autenticación no cifrados en los archivos donde estén almacenados, y así utilizar los datos para obtener acceso no autorizado.
	8.3.2.b Evalúe los repositorios de los factores de autenticación para verificar que son ilegibles durante el almacenamiento.	
Objetivo del Enfoque Personalizado	**8.3.2.c** Evalúe transmisiones de datos para verificar que los factores de autenticación son ilegibles durante la transmisión.	
Los factores de autenticación legibles no pueden obtenerse, derivarse o reutilizarse a partir de la interceptación de comunicaciones o de datos almacenados.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
8.3.3 La identidad del usuario se verifica antes de modificar cualquier factor de autenticación.	**8.3.3** Evalúe los procedimientos para modificar los factores de autenticación y observe al personal de seguridad para verificar que cuando un usuario solicita la modificación de un factor de autenticación, se verifica la identidad del usuario antes de modificar el factor de autenticación.	**Objetivo** Los individuos malintencionados utilizan técnicas de "ingeniería social" para hacerse pasar por usuarios del sistema -por ejemplo, llamando a un servicio de asistencia y actuando como un usuario legítimo- para que se cambie un factor de autenticación y así poder utilizar un ID de usuario válido. Exigir la identificación positiva de un usuario reduce la probabilidad de éxito de este tipo de ataques. **Buenas Prácticas** Las modificaciones de los factores de autenticación para los que debe verificarse la identidad del usuario incluyen, entre otras cosas, el restablecimiento de contraseñas, proveer nuevos *token, hardware* o *software,* y generar nuevas claves. **Ejemplos** Los métodos para verificar la identidad de un usuario incluyen una pregunta/respuesta secreta, información basada en el conocimiento, y llamar al usuario a un número de teléfono conocido y previamente establecido.
Objetivo del Enfoque Personalizado		
Las personas no autorizadas no pueden obtener acceso al sistema suplantando la identidad de un usuario autorizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **8.3.4** Los intentos de autenticación inválidos se limitan mediante: • El bloqueo del ID de usuario después de no más de 10 intentos. • El establecimiento de la duración del bloqueo a un mínimo de 30 minutos o hasta que se confirme la identidad del usuario. **Objetivo del Enfoque Personalizado** Los factores de autenticación no pueden ser adivinados durante un ataque en línea de fuerza bruta. **Notas de Aplicabilidad** Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los *IDs* utilizados por los cajeros en los terminales de punto de venta).	**Procedimientos de Prueba del Enfoque Definido** **8.3.4.a** Evalúe los ajustes de configuración del sistema para verificar que los parámetros de autenticación están configurados para requerir que las cuentas del usuario se bloqueen después de no más de 10 intentos de inicio de sesión inválidos. **8.3.4.b** Evalúe los ajustes de configuración del sistema para verificar que los parámetros de contraseña están establecidos para requerir que, una vez que una cuenta de usuario es bloqueada, esta permanezca bloqueada por un mínimo de 30 minutos o hasta que la identidad del usuario sea confirmada.	**Objetivo** Sin mecanismos de bloqueo de cuentas, un atacante puede intentar continuamente adivinar una contraseña a través de herramientas manuales o automáticas (como, por ejemplo, el "cracking" de contraseñas) hasta que el atacante tenga éxito y obtenga acceso a la cuenta de un usuario. Si una cuenta se bloquea debido a que alguien intenta continuamente adivinar la contraseña, los controles para retrasar la reactivación de la cuenta bloqueada impiden que individuos malintencionados adivinen la contraseña, ya que tendrán que esperar un mínimo de 30 minutos para que la cuenta se reactive. **Buenas Prácticas** Antes de reactivar una cuenta bloqueada, se debe confirmar la identidad del usuario. Por ejemplo, el administrador o el personal de asistencia pueden validar que el propietario real de la cuenta es el que solicita la reactivación, o puede haber mecanismos de autoservicio de restablecimiento de contraseñas que el propietario de la cuenta utiliza para verificar su identidad.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.3.5 Si las contraseñas/frases de paso se utilizan como factores de autenticación para cumplir con el requisito 8.3.1, estas se establecen y restablecen para cada usuario tal y como sigue: • Se establecen a un valor único para la primera vez que se utilizan y al restablecerse. • Existe la obligatoriedad de cambiarlos inmediatamente después del primer uso.	**8.3.5** Evalúe los procedimientos para establecer y restablecer las contraseñas/frases de paso (si se utilizan como factores de autenticación para cumplir con el Requisito 8.3.1) y observe al personal de seguridad para verificar que las contraseñas/frases de paso se establecen y restablecen de acuerdo con todos los elementos especificados en este requisito.	Si se utiliza la misma contraseña/frase de paso para cada nuevo usuario, un usuario interno, un antiguo empleado o individuos malintencionados pueden conocer o descubrir fácilmente el valor y utilizarlo para obtener acceso a la cuenta antes de que el usuario autorizado intente utilizar la contraseña.
Objetivo del Enfoque Personalizado		
Una contraseña/frase de paso inicial o restablecida asignada a un usuario no puede ser utilizada por otro usuario no autorizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.3.6 Si las contraseñas/frases de paso se utilizan como factores de autenticación para cumplir el requisito 8.3.1, estas deberán cumplir el siguiente nivel mínimo de complejidad: • Una longitud mínima de 12 caracteres (o SI el sistema no admite 12 caracteres, una longitud mínima de ocho caracteres). • Contener tanto caracteres numéricos como alfabéticos.	**8.3.6** Evalúe los ajustes de configuración de los sistemas para verificar que los parámetros de complejidad de las contraseñas/frase de paso de los usuarios estén establecidos de acuerdo con todos los elementos especificados en este requisito.	Las contraseñas/frases de paso robustas pueden ser la primera línea de defensa en una red, ya que individuos maliciosos a menudo tratarán primero de encontrar cuentas con contraseñas débiles, estáticas o inexistentes. Si las contraseñas son cortas o fáciles de adivinar, resulta relativamente fácil para individuos malintencionados encontrar esas cuentas débiles y comprometer una red bajo la apariencia de una identificación de usuario válida. **Buenas Prácticas** La fortaleza de la contraseña/frase de paso depende de la complejidad, longitud y aleatoriedad de la misma. Las contraseñas/frases de paso deben de ser lo suficientemente complejas como para que un atacante no pueda adivinarlas o descubrir su valor. Las entidades pueden considerar la posibilidad de aumentar la complejidad exigiendo el uso de caracteres especiales y de mayúsculas y minúsculas, además de los estándares mínimos indicados en este requisito. La complejidad adicional aumenta el tiempo requerido necesario para los ataques de fuerza bruta fuera de línea contra “*hashes*” de contraseñas/frases de paso. Otra opción para aumentar la resistencia de las contraseñas a los ataques de adivinación es comparar las contraseñas/frases de paso propuestas con las de una lista de contraseñas “malas”, de modo que los usuarios empleen nuevas contraseñas para cualquier contraseña encontrada en la lista.
Objetivo del Enfoque Personalizado		
Una contraseña/frase de paso adivinada no puede ser verificada por un ataque de fuerza bruta en línea o fuera de línea.		
Notas de Aplicabilidad		
Este requisito no se aplica a: • Cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los *IDs* utilizados por los cajeros en los terminales de punto de venta). • Cuentas de aplicaciones o sistemas, que se rigen por los requisitos de la sección 8.6. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* Hasta el 31 de marzo de 2025, las contraseñas deben tener una longitud mínima de siete caracteres, de acuerdo con el requisito 8.2.3 PCI DSS v3.2.1.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **8.3.7** Las personas no pueden enviar una nueva contraseña / frase de paso que sea igual a cualquiera de las últimas cuatro contraseñas / frases de paso utilizadas. **Objetivo del Enfoque Personalizado** No se puede utilizar una contraseña utilizada anteriormente para obtener acceso a una cuenta al menos durante 12 meses. **Notas de Aplicabilidad** Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los *IDs* utilizados por los cajeros en los terminales de punto de venta).	**Procedimientos de Prueba del Enfoque Definido** **8.3.7** Evalúe los ajustes de configuración de los sistemas para verificar que los parámetros de contraseñas estén configurados para requerir que las nuevas contraseñas/frases de paso no puedan ser las mismas que las cuatro contraseñas/frases de paso utilizadas anteriormente.	**Objetivo** Si no se mantiene el historial de las contraseñas, la eficacia de cambiar las contraseñas se reduce, ya que las contraseñas anteriores se pueden reutilizar una y otra vez. Exigir que las contraseñas no se puedan reutilizar durante un período reduce la probabilidad de que las contraseñas adivinadas, u obtenidas mediante fuerza bruta se vuelvan a utilizar en el futuro. Es posible que las contraseñas o frases de paso se hayan cambiado previamente debido a la sospecha de que estén comprometidas o porque la contraseña o frase de paso excedió su período de uso efectivo; por ambas razones las contraseñas utilizadas anteriormente no deben reutilizarse.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.3.8 Las políticas y los procedimientos de autenticación están documentados y son comunicados a todos los usuarios, incluyendo: • Orientación sobre la selección de factores de autenticación robustos. • Orientación sobre cómo los usuarios deben proteger sus factores de autenticación. • Instrucciones para no reutilizar contraseñas/frases de paso utilizadas anteriormente. • Instrucciones para cambiar contraseñas/frases de paso si existe alguna sospecha o conocimiento de que la contraseña/frase de paso se ha visto comprometida y cómo reportar el incidente.	**8.3.8.a** Evalúe los procedimientos y entreviste al personal para verificar que las políticas y los procedimientos de autenticación se distribuyan a todos los usuarios.	Comunicar las políticas y los procedimientos de autenticación a todos los usuarios les ayuda a comprender y cumplir las políticas. **Buenas Prácticas** La orientación sobre la selección de contraseñas seguras puede incluir sugerencias para ayudar al personal a seleccionar contraseñas difíciles de adivinar que no contienen palabras del diccionario o información sobre el usuario, como el ID del usuario, los nombres de los miembros de la familia, la fecha de nacimiento, etc. La guía para proteger los factores de autenticación puede incluir el no anotar contraseñas o no guardarlas en archivos inseguros, y estar alerta a personas malintencionadas que puedan intentar explotar sus contraseñas (como por ejemplo, a través de una llamada a un empleado solicitando su contraseña para que la persona que llama pueda " resolver un problema"). Alternativamente, las entidades pueden implementar procesos para confirmar que las contraseñas cumplen con las políticas de contraseñas, por ejemplo, comparando las opciones de contraseñas con una lista de contraseñas inaceptables y haciendo que los usuarios elijan una nueva contraseña para cualquiera que coincida con una de la lista. Instruir a los usuarios para que cambien las contraseñas si existe la posibilidad de que la contraseña ya no sea segura puede evitar que usuarios malintencionados utilicen una contraseña legítima para obtener acceso no autorizado.
Objetivo del Enfoque Personalizado	**8.3.8.b** Revise las políticas y los procedimientos de autenticación que se distribuyen a los usuarios y verifique que incluyan los elementos especificados en este requisito.	
Los usuarios están bien informados sobre el uso correcto de los factores de autenticación y pueden acceder a asistencia y orientación cuando sea necesario.	**8.3.8.c** Entreviste a los usuarios para verificar que están familiarizados con las políticas y los procedimientos de autenticación.	

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **8.3.9** Si las contraseñas/frases de paso se utilizan como el único factor de autenticación para el acceso del usuario (es decir, en cualquier implementación de autenticación de factor único), entonces: • Las contraseñas/frases de paso se cambian al menos una vez cada 90 días, **O** • La postura de seguridad de las cuentas se analiza dinámicamente y el acceso a los recursos en tiempo real se determina automáticamente de acuerdo a dicha postura de seguridad. **Objetivo del Enfoque Personalizado** Una contraseña/frase de paso que esté comprometida y no haya sido detectada, no se puede utilizar de forma indefinida.	**Procedimientos de Prueba del Enfoque Definido** **8.3.9** Si las contraseñas/frases de paso se utilizan como el único factor de autenticación para el acceso de los usuarios, inspeccione los ajustes de configuración de los sistemas para verificar que las contraseñas/frases de paso se administran de acuerdo con UNO de los elementos especificados en este requisito.	**Objetivo** El acceso a los componentes del sistema dentro del alcance, que no están en el CDE, se puede proporcionar mediante un solo factor de autenticación, tal como una contraseña/frase de paso, un dispositivo *token* o tarjeta inteligente, o un atributo biométrico. Cuando se emplean contraseñas/frases de paso como el único factor de autenticación para dicho acceso, se requieren controles adicionales para proteger la integridad de la contraseña/frase de paso. **Buenas Prácticas** Las contraseñas/frases de paso que son válidas durante mucho tiempo sin cambios brindan a individuos malintencionados más tiempo para violarlas. Cambiar las contraseñas periódicamente ofrece menos tiempo para que individuos malintencionados averigüen las contraseñas/frases de paso y menos tiempo para usar una contraseña que esté comprometida. El uso de una contraseña/frase de paso como único factor de autenticación proporciona un único punto de fallo si esta se ve comprometida. Por lo tanto, en estas implementaciones, se necesitan controles para minimizar la duración de la actividad maliciosa a través de una contraseña/frase de paso que esté comprometida. El análisis dinámico de la postura de seguridad de una cuenta es otra opción que permite la detección y rápida respuesta para abordar las credenciales potencialmente comprometidas. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito se aplica a los componentes del sistema dentro del alcance que no están en el CDE ya que esos componentes no están sujetos a los requisitos de los MFA. Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción (como los *IDs* utilizados por los cajeros en los terminales de punto de venta). Este requisito no se aplica a las cuentas de clientes de proveedores de servicios, pero se aplica a las cuentas del personal del proveedor de servicios.		Dicho análisis consume varios puntos, que pueden incluir la integridad del dispositivo, la ubicación, el número de accesos y los recursos a los que se accede, para determinar en tiempo real si se puede otorgar a una cuenta, el acceso a un recurso solicitado. De esta manera, se puede denegar el acceso y bloquear las cuentas si se sospecha que las credenciales de autenticación se han visto comprometidas. **Información Adicional** Para obtener información sobre el uso del análisis dinámico para administrar el acceso de los usuarios a los recursos, consulte NIST SP 800-207 *Zero Trust Architecture.*
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** El uso de una contraseña/frase de paso como único factor de autenticación proporciona un único punto de fallo si esta se ve comprometida. Por lo tanto, en estas implementaciones, se necesitan controles para minimizar la duración de la actividad maliciosa a través de una contraseña/frase de paso que esté comprometida. **Buenas Prácticas** Las contraseñas/frases de paso que son válidas durante mucho tiempo sin cambios brindan a individuos malintencionados más tiempo para violar la contraseña/frase. Cambiar las contraseñas periódicamente ofrece menos tiempo para que individuos malintencionados averigüen las contraseñas/frases de paso y menos tiempo para usar las contraseñas que estén comprometidas.
8.3.10 ***Requisito adicional solo para proveedores de servicios:*** Si las contraseñas / frases de paso contraseña se utilizan como el único factor de autenticación para el acceso del usuario del cliente a los datos del titular de la tarjeta (es decir, en cualquier implementación de autenticación de factor único), entonces se brinda orientación a los usuarios del cliente, que incluye: • Orientación para que los clientes cambien sus contraseñas/frases de paso periódicamente. • Orientación sobre cuándo y bajo qué circunstancias se cambian las contraseñas/frases de paso. *(continúa en la página siguiente)*	**8.3.10** ***Procedimiento de prueba adicional sólo para evaluaciones de proveedores de servicios:*** Si se utilizan contraseñas/frases de paso como el único factor de autenticación para el acceso del usuario del cliente a los datos del titular de la tarjeta, examine la guía proporcionada a los usuarios del cliente para verificar que la guía incluye todos los elementos especificados en este requisito.	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Las contraseñas/frases de paso de los clientes de proveedores de servicios no se pueden utilizar de forma indefinida. **Notas de Aplicabilidad** Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios. Este requisito no aplica para cuentas de usuarios consumidores que acceden a la información de su propia tarjeta de pago. Este requisito para los proveedores de servicios será reemplazado por el Requisito 8.3.10.1 una vez que el 8.3.10.1 entre en vigor.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **8.3.10.1** ***Requisito adicional sólo para proveedores de servicios:*** Si las contraseñas/frases de paso se utilizan como el único factor de autenticación para el acceso del usuario del cliente (es decir, en cualquier implementación de autenticación de factor único), entonces: • Las contraseñas/frases de paso se cambian al menos una vez cada 90 días, **O** • La postura de seguridad de las cuentas se analiza dinámicamente y el acceso a los recursos en tiempo real se determina automáticamente de acuerdo a dicha postura. **Objetivo del Enfoque Personalizado** Las contraseñas/frases de paso de los clientes de proveedores de servicios no se pueden utilizar de forma indefinida. **Notas de Aplicabilidad** Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios. Este requisito no se aplica a las cuentas de los usuarios consumidores que acceden a la información de sus propias tarjetas de pago. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* Hasta que este requisito entre en vigor el 31 de marzo de 2025, los proveedores de servicios pueden cumplir con el Requisito 8.3.10 o el 8.3.10.1.	**Procedimientos de Prueba del Enfoque Definido** **8.3.10.1** ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Si se utilizan contraseñas/frases de paso como único factor de autenticación para el acceso de los usuarios del cliente, inspeccionar los ajustes de configuración de los sistemas para verificar que las contraseñas/frases de paso se gestionan de acuerdo a UNO de los elementos especificados en este requisito.	**Objetivo** El uso de una contraseña/frase de paso como único factor de autenticación proporciona un único punto de fallo si esta se ve comprometida. Por lo tanto, en estas implementaciones, se necesitan controles para minimizar la duración de la actividad maliciosa a través de una contraseña/frase de paso que esté comprometida. **Buenas Prácticas** Las contraseñas/frases de paso que son válidas durante mucho tiempo sin cambios brindan a individuos malintencionados más tiempo para violar la contraseña/frase. Cambiar las contraseñas periódicamente ofrece menos tiempo para que individuos malintencionados averigüen las contraseñas/frases de paso y menos tiempo para usar las contraseñas que estén comprometidas. El análisis dinámico de la postura de seguridad de una cuenta es otra opción que permite la detección y rápida respuesta para abordar las credenciales potencialmente comprometidas. Dicho análisis consume varios puntos, que pueden incluir la integridad del dispositivo, la ubicación, el número de accesos y los recursos a los que se accede para determinar en tiempo real si se puede otorgar a una cuenta, el acceso a un recurso solicitado. De esta manera, se puede denegar el acceso y bloquear las cuentas si se sospecha que las credenciales de autenticación se han visto comprometidas. **Información Adicional** Para obtener información sobre el uso del análisis dinámico para administrar el acceso de los usuarios a los recursos, consulte *NIST SP 800-207 Arquitectura Zero Trust.*

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
8.3.11 Cuando se utilizan factores de autenticación como *tokens* de seguridad físicos o lógicos, tarjetas inteligentes o certificados: • Los factores se asignan a un usuario individual y no se comparten entre varios usuarios. • Los controles físicos y/o lógicos garantizan que sólo el usuario previsto pueda utilizar ese factor para acceder.	**8.3.11.a** Evalúe las políticas y los procedimientos de autenticación para verificar que los procedimientos para utilizar factores de autenticación tales como *tokens* de seguridad físicos, tarjetas inteligentes y certificados están definidos e incluyen todos los elementos especificados en este requisito.	**Objetivo** Si múltiples usuarios pueden utilizar factores de autenticación como *tokens*, tarjetas inteligentes y certificados, puede resultar imposible identificar al individuo que utiliza el mecanismo de autenticación. **Buenas Prácticas** Disponer de controles físicos y/o lógicos (por ejemplo, un PIN, datos biométricos o una contraseña) para autenticar de forma única al usuario de la cuenta impedirá que usuarios no autorizados puedan ganar acceso a la cuenta del usuario mediante el uso de un factor de autenticación compartido.
	8.3.11.b Entreviste al personal de seguridad para verificar que los factores de autenticación se asignan a un usuario individual y no se comparten entre varios usuarios.	
Objetivo del Enfoque Personalizado	**8.3.11.c** Evalúe los ajustes de configuración de los sistemas y/o observe los controles físicos, según corresponda, para verificar que los controles se implementan para garantizar que sólo el usuario previsto puede utilizar ese factor para obtener acceso.	
Un factor de autenticación no puede ser utilizado por nadie más que por el usuario al que se le ha asignado.		

Requisitos y Procedimientos de Prueba		Guía
8.4 Se implementa la autenticación múltiples factores (MFA) para proteger el acceso al CDE.		
Requisitos del Enfoque Definido **8.4.1** Los MFA se implementan para todos los accesos al CDE sin consola, para el personal con acceso administrativo. **Objetivo del Enfoque Personalizado** El acceso administrativo al CDE no puede obtenerse mediante el uso de un factor de autenticación único. **Notas de Aplicabilidad** El requisito de MFA para el acceso administrativo sin consola se aplica a todo el personal con privilegios elevados o aumentados que accede al CDE a través de una conexión sin consola, es decir, a través de un acceso lógico que se produce a través de una interfaz de red en lugar de una conexión directa y física. Los MFA se consideran una práctica recomendada para el acceso administrativo sin consola, a los componentes del sistema en cuestión que no forman parte del CDE.	**Procedimientos de Prueba del Enfoque Definido** **8.4.1.a** Evalúe las configuraciones de la red y/o del sistema para verificar que se requieren MFA para todos los accesos al CDE sin consola, para el personal con acceso administrativo. **8.4.1.b** Observe al personal administrador que ingresa al CDE y verifique que los MFA son requeridos.	**Objetivo** Solicitar más de un tipo de factor de autenticación reduce la probabilidad de que el atacante pueda ingresar a un sistema haciéndose pasar por un usuario legítimo, ya que el atacante necesitaría comprometer varios factores de autenticación. Esto es especialmente cierto en entornos en los que tradicionalmente el único factor de autenticación empleado era algo que el usuario conoce, como una contraseña o una frase de paso. **Definiciones** Usar un factor dos veces (por ejemplo, usar dos contraseñas separadas) no se considera autenticación multifactorial.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.4.2 Los MFA se implementan para todos los accesos al CDE.	**8.4.2.a** Evalúe la red yo las configuraciones del sistema para verificar que los MFA estén implementados para todos los accesos al CDE.	Solicitar más de un tipo de factor de autenticación reduce la probabilidad de que el atacante pueda ingresar a un sistema haciéndose pasar por un usuario legítimo, ya que el atacante necesitaría comprometer varios factores de autenticación. Esto es especialmente cierto en entornos en los que tradicionalmente el único factor de autenticación empleado era algo que el usuario conoce, como una contraseña o una frase de paso.
Objetivo del Enfoque Personalizado	**8.4.2.b** Observe al personal que ingresa al CDE y examine la evidencia para verificar que los MFA son requeridos.	**Definiciones**
El acceso al CDE no se puede obtener mediante el uso de un solo factor de autenticación.		Usar un factor dos veces (por ejemplo, usar dos contraseñas separadas) no se considera autenticación multifactorial.
Notas de Aplicabilidad		
Este requisito no se aplica a: • Aplicación o cuentas del sistema que desempeñan funciones automatizadas. • Cuentas de usuario en terminales de punto de venta que tienen acceso a un solo número de tarjeta a la vez para facilitar una sola transacción (como las IDs utilizadas por los cajeros en terminales de punto de venta). Se requieren los MFA para ambos tipos de accesos especificados en los Requisitos 8.4.2 y 8.4.3. Por lo tanto, la aplicación de los MFA a un tipo de acceso no reemplaza la necesidad de aplicar otra instancia de MFA al otro tipo de acceso. Si una persona se conecta primero a la red de la entidad a través de un acceso remoto, y luego inicia una conexión al CDE desde dentro de la red; según este requisito, la persona se autenticaría usando los MFA dos veces, una cuando se conecta a través de acceso remoto a la red de la entidad, y luego cuando se conecta a través de un acceso administrativo sin consola desde la red de la entidad al CDE. *(continúa en la página siguiente)*		

Requisitos y Procedimientos de Prueba		Guía
Se requieren los MFA para ambos tipos de accesos especificados en los Requisitos 8.4.2 y 8.4.3. Por lo tanto, la aplicación de los MFA a un tipo de acceso no reemplaza la necesidad de aplicar otra instancia de MFA al otro tipo de acceso. Si una persona se conecta primero a la red de la entidad a través de un acceso remoto, y luego inicia una conexión al CDE desde dentro de la red; según este requisito, la persona se autenticaría usando los MFA dos veces, una cuando se conecta a través de acceso remoto a la red de la entidad, y luego cuando se conecta a través de un acceso administrativo sin consola desde la red de la entidad al CDE. *Los requisitos de los MFA se aplican a todos los tipos de componentes del sistema, incluyendo la nube, los sistemas alojados y las aplicaciones locales, los dispositivos de seguridad de red, las estaciones de trabajo, los servidores y los puntos finales, e incluye el acceso directo a las redes o sistemas de una entidad, así como el acceso basado en web a una aplicación o función.* *Los MFA para acceso remoto al CDE se pueden implementar a nivel de red o sistema/aplicación; no es necesario que se apliquen en ambos niveles. Por ejemplo, si se usan MFA cuando un usuario se conecta a la red del CDE, no es necesario que se usen cuando el usuario inicia sesión en cada sistema o aplicación dentro del CDE.* *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **8.4.3** Los MFA se implementan para todos los accesos a redes remotas que se originan fuera de la red de la entidad y que podrían ingresar o impactar el CDE de la siguiente manera: • Todo acceso remoto por parte de todo el personal, tanto usuarios como administradores, originados fuera de la red de la entidad. • Todo acceso remoto por terceros y proveedores. **Objetivo del Enfoque Personalizado** No se puede obtener acceso remoto a la red de la entidad mediante el uso de un solo factor de autenticación. **Notas de Aplicabilidad** El requisito de los MFA para el acceso remoto que se origina desde fuera de la red de la entidad se aplica a todas las cuentas de usuario que pueden ingresar a la red de forma remota, donde ese acceso remoto conduce o podría conducir a un acceso al CDE. Si el acceso remoto se realiza a una parte de la red de la entidad que está correctamente segmentada del CDE, de manera que los usuarios remotos no puedan ingresar al CDE o afectarlo, no se requiere MFA para el acceso remoto a esa parte de la red. Sin embargo, se requieren los MFA para cualquier acceso remoto a redes con acceso al CDE y se recomienda para todos los accesos remotos a las redes de la entidad. *(continúa en la página siguiente)*	**Procedimientos de Prueba del Enfoque Definido** **8.4.3.a** Evalúe la red y/o las configuraciones del sistema para los servidores y sistemas de acceso remoto para verificar que se requieran MFA de acuerdo con todos los elementos especificados en este requisito. **8.4.3.b** Observe al personal (por ejemplo, usuarios y administradores) que se conectan de forma remota a la red y verifique que se requiera autenticación multifactorial.	**Objetivo** Requerir más de un tipo de factor de autenticación reduce la probabilidad de que un atacante pueda obtener acceso a un sistema haciéndose pasar por un usuario legítimo, porque el atacante necesitaría comprometer múltiples factores de autenticación. Esto es especialmente cierto en entornos donde tradicionalmente el factor de autenticación único empleado era algo que el usuario conoce, como una contraseña o una frase de contraseña. **Definiciones** La autenticación multifactorial (MFA) requiere que una persona presente un mínimo de dos de los tres factores de autenticación especificados en el Requisito 8.3.1 antes de que se otorgue el acceso. Usar un factor dos veces (por ejemplo, usar dos contraseñas separadas) no se considera autenticación multifactorial.

Requisitos y Procedimientos de Prueba		Guía
Los requisitos de los MFA se aplican a todos los tipos de componentes del sistema, incluyendo la nube, los sistemas alojados y las aplicaciones locales, los dispositivos de seguridad de red, las estaciones de trabajo, los servidores y los puntos finales, e incluye el acceso directo a las redes o sistemas de una entidad, así como el acceso basado en web a una aplicación o función.		

Requisitos y Procedimientos de Prueba		Guía
8.5 Los sistemas de autenticación de múltiples factores (MFA) están configurados para evitar su uso indebido.		
Requisitos del Enfoque Definido **8.5.1** Los sistemas MFA se implementan de la siguiente manera: • El sistema MFA no es susceptible a ataques de repetición. • Los sistemas MFA no pueden ser omitidos por ningún usuario, incluyendo los usuarios administrativos, a menos que esté específicamente documentado y autorizado por la administración de manera excepcional durante un período de tiempo limitado. • Se utilizan al menos dos tipos diferentes de factores de autenticación. • Se requiere el éxito de todos los factores de autenticación antes de que se otorgue el acceso. **Objetivo del Enfoque Personalizado** Los sistemas MFA son resistentes a los ataques y controlan estrictamente cualquier invalidación administrativa. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba del Enfoque Definido** **8.5.1.a** Evalúe la documentación del sistema del proveedor para verificar que el sistema MFA no sea susceptible a ataques de repetición. **8.5.1.b** Evalúe las configuraciones del sistema para la implementación de los MFA a fin de verificar que está configurado de acuerdo con todos los elementos especificados en este requisito. **8.5.1.c** Entreviste al personal responsable y observe los procesos para verificar que cualquier solicitud de evadir los MFA sea específicamente documentada y autorizada por la dirección, como algo excepcional y por un período de tiempo limitado. **8.5.1.d** Observe al personal que inicia sesión en los componentes del sistema en el CDE para verificar que el acceso se otorgue sólo después de que todos los factores de autenticación sean exitosos. **8.5.1.e** Observe al personal que se conecta de forma remota desde fuera de la red de la entidad para verificar que el acceso se otorgue sólo después de que todos los factores de autenticación sean exitosos.	**Objetivo** Los atacantes pueden evitar los sistemas MFA mal configurados. Por lo tanto, este requisito aborda la configuración de los sistemas MFA que brindan los MFA a los usuarios que acceden a los componentes del sistema en el CDE. **Definiciones** Usar un tipo de factor dos veces (por ejemplo, usar dos contraseñas separadas) no se considera autenticación multifactorial. **Información Adicional** Para obtener más información sobre los sistemas y las funciones de los MFA, consulte lo siguiente: Información Complementaria PCI SCC: Autenticación Multi-Factorial Preguntas Frecuentes *(FAQ)* PCI SCC sobre este tema.

Requisitos y Procedimientos de Prueba		Guía
8.6 El uso de cuentas de aplicaciones y sistemas y factores de autenticación asociados se gestiona estrictamente.		
Requisitos del Enfoque Definido **8.6.1** Si las cuentas utilizadas por los sistemas o aplicaciones pueden ser utilizadas para el inicio de sesión interactivo, se gestionan de la siguiente manera: • Se impide el uso interactivo a menos que se requiera por una circunstancia excepcional. • El uso está limitado al tiempo necesario para la circunstancia excepcional. • La justificación de negocio para su uso está documentada. • El uso interactivo está explícitamente aprobado por la dirección. • La identidad del usuario individual se confirma antes de que se conceda el acceso a una cuenta. • Cada acción realizada es atribuible a un usuario individual **Objetivo del Enfoque Personalizado** Cuando se utilizan de forma interactiva, todas las acciones con las cuentas designadas como cuentas de sistema o de aplicación están autorizadas y son atribuibles a personas individualmente. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba del Enfoque Definido** **8.6.1** Evalúe las cuentas de la aplicación y del sistema que pueden ser usadas de forma interactiva y entreviste al personal administrativo para verificar que las cuentas de la aplicación y del sistema son administradas de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Al igual que las cuentas de usuarios individuales, las cuentas del sistema y de la aplicación requieren responsabilidad y una gestión estricta para garantizar que se utilicen solo para el propósito previsto y no se utilicen de forma indebida. Los atacantes a menudo ponen en peligro las cuentas del sistema o de las aplicaciones para obtener acceso a los datos de titulares de tarjetas. **Buenas Prácticas** Siempre que sea posible, configure las cuentas del sistema y de la aplicación para impedir un inicio de sesión interactivo y así evitar que personas no autorizadas inicien sesión y usen la cuenta con sus privilegios de sistema asociados, y para limitar las máquinas y dispositivos en los que se puede usar la cuenta. **Definiciones** Las cuentas del sistema o de la aplicación son aquellas cuentas que ejecutan procesos o realizan tareas en un sistema informático o una aplicación y no suelen ser cuentas en las que una persona inicia sesión. Esas cuentas suelen tener privilegios elevados requeridos para realizar tareas o funciones especializadas. El inicio de sesión interactivo es la capacidad de una persona para iniciar sesión en una cuenta de sistema o aplicación de la misma manera que una cuenta de usuario normal. El uso de las cuentas del sistema y de la aplicación de esta manera significa que no hay responsabilidad y trazabilidad de las acciones realizadas por el usuario.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
8.6.2 Las contraseñas/frases de paso para cualquier aplicación y cuentas de sistema que puedan ser utilizadas para el inicio de sesión interactivo no están codificadas en scripts, archivos de configuración/propiedades, o código fuente a la medida y personalizado.	**8.6.2.a** Entreviste al personal y examine los procedimientos de desarrollo del sistema para verificar que los procesos están definidos para las cuentas de la aplicación y del sistema que pueden utilizarse para iniciar sesiones interactivas, especificando que las contraseñas/frases de paso no están codificadas en scripts, archivos de configuración/propiedades o código fuente a la medida y personalizado.	No proteger adecuadamente las contraseñas/frases de paso utilizadas por las cuentas de aplicaciones y sistemas, especialmente si esas cuentas pueden utilizarse para el inicio de sesión interactivo, aumenta el riesgo y el éxito del uso no autorizado de esas cuentas privilegiadas. **Buenas Prácticas** La modificación de estos valores por sospecha o confirmación de divulgación puede ser especialmente difícil de aplicar. Las herramientas pueden facilitar tanto la gestión como la seguridad de los factores de autenticación para las cuentas de aplicaciones y sistemas. Por ejemplo, considere las bóvedas de contraseñas u otros controles gestionados por el sistema.
Objetivo del Enfoque Personalizado Las contraseñas/frases de paso utilizadas por las cuentas de aplicaciones y sistemas no pueden ser utilizadas por personal no autorizado.	**8.6.2.b** Evalúe los scripts, archivos de configuración/propiedades, y el código fuente personalizado y a la medida para las cuentas de aplicación y sistema que pueden ser utilizadas para iniciar sesiones interactivas, a fin de verificar que las contraseñas/frases de paso para esas cuentas no están presentes.	
Notas de Aplicabilidad Las contraseñas/frases de acceso almacenadas deben estar cifradas de acuerdo con el Requisito 8.3.2 PCI DSS. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Las cuentas de sistemas y aplicaciones plantean un riesgo de seguridad más inherente que las cuentas de usuario, ya que a menudo se ejecutan en un contexto de alta seguridad, con acceso a sistemas que no suelen concederse a las cuentas de usuario, como el acceso programático a las bases de datos, etc. Por lo tanto, se debe prestar especial atención a la protección de las contraseñas/frases de paso utilizadas para las cuentas de aplicaciones y sistemas. **Buenas Prácticas** Las entidades deben tener en cuenta los siguientes factores de riesgo a la hora de determinar cómo proteger del uso indebido, las contraseñas/frases de paso de las aplicaciones y sistemas: • ¿Qué tan seguro es el almacenamiento de las contraseñas/frases de acceso? (por ejemplo, si se almacenan en una bóveda de contraseñas). • Rotación del personal. • El número de personas con acceso al factor de autenticación. • Si la cuenta puede utilizarse para inicio de sesiones interactivas. • Si la postura de seguridad de las cuentas es analizada dinámicamente, y el acceso en tiempo real a los recursos se determina automática y consecuentemente (ver el Requisito 8.3.9). Todos estos elementos afectan al nivel de riesgo de las cuentas de aplicación y de sistema y podrían afectar la seguridad de los sistemas a los que acceden las cuentas de sistema y de aplicación. *(continúa en la página siguiente)*
8.6.3 Las contraseñas/frases de paso para cualquier cuenta de aplicación y de sistema están protegidas contra el uso indebido de la siguiente manera: • Las cuentas de sistema y de aplicación se cambian periódicamente, (a una frecuencia definida en el análisis de riesgos específico de la entidad, el cual se desarrolla de acuerdo a todos los elementos especificados en el Requisito 12.3.1.) y ante la sospecha o la confirmación de que estén comprometidas. • Las contraseñas/frases de acceso se construyen con la complejidad necesaria y apropiada para la frecuencia con la que la entidad cambia las contraseñas/frases de acceso.	**8.6.3.a** Evalúe las políticas y los procedimientos para verificar que estén definidos para proteger las contraseñas/frases de paso de las cuentas de aplicaciones o sistemas contra el uso indebido de acuerdo con todos los elementos especificados en este requisito. **8.6.3.b** Evalúe el análisis de riesgo específico de la entidad para el cambio, frecuencia y complejidad de las contraseñas/frases de paso utilizadas para conexiones interactivas a las cuentas de aplicaciones o sistemas para verificar que se realizó un análisis de riesgo con todos los elementos especificados en el Requisito 12.3.1 y direcciones: • La frecuencia definida para los cambios periódicos de las contraseñas/frases de paso de las aplicaciones y sistemas. • La complejidad definida para las contraseñas/frases de acceso y la adecuación de la complejidad en relación con la frecuencia de los cambios.	
Objetivo del Enfoque Personalizado Las contraseñas/frases de acceso utilizadas por las cuentas de aplicación y del sistema no pueden utilizarse indefinidamente y están estructuradas para resistir ataques de fuerza bruta y de adivinación.	**8.6.3.c** Entreviste al personal responsable y examine los ajustes de configuración del sistema para verificar que las contraseñas/frases de paso para cualquier aplicación y cuentas del sistema que puedan utilizarse para el inicio de sesiones interactivas estén protegidas contra el uso indebido de acuerdo con todos los elementos especificados en este requisito.	
Notas de Aplicabilidad *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
		Las entidades deben correlacionar su frecuencia de cambio seleccionada para las contraseñas/contraseñas de aplicaciones y sistemas con su complejidad seleccionada para esas contraseñas/frases de contraseña - es decir, la complejidad debe ser más rigurosa cuando las contraseñas/frases de contraseña se cambian con poca frecuencia y puede ser menos rigurosa cuando se cambian con más frecuencia. Por ejemplo, una mayor frecuencia de cambio está más justificada cuando la complejidad de las contraseñas/frases de paso se establece en 36 caracteres alfanuméricos con letras mayúsculas y minúsculas, números y caracteres especiales. Las mejores prácticas son considerar los cambios de contraseña al menos una vez al año, una longitud de contraseña/frase de paso de al menos 15 caracteres, y una complejidad para las contraseñas/frase de paso de caracteres alfanuméricos, con letras mayúsculas y minúsculas, y caracteres especiales. **Información Adicional** Para obtener información sobre la variabilidad y la equivalencia de la fuerza de las contraseñas para contraseñas/frases de contraseña de diferentes formatos, consulte los estándares del sector (por ejemplo, la versión actual de las *Directrices de Identidad Digital NIST SP 800-63*).

Requisito 9: Restringir el Acceso Físico a los Datos de Tarjetahabientes

Secciones	
9.1	Los procesos y mecanismos para restringir el acceso físico a los datos de titulares de tarjetas están definidos y comprendidos.
9.2	Los controles de acceso físico gestionan la entrada a las instalaciones y sistemas que contienen datos de titulares de tarjetas.
9.3	El acceso físico del personal y de los visitantes está autorizado y gestionado.
9.4	Los medios con datos de titulares de tarjetas se almacenan, acceden, distribuyen y destruyen de forma segura.
9.5	Los dispositivos de punto de interacción (POI) están protegidos contra manipulaciones y sustituciones no autorizadas.

Descripción

Cualquier acceso físico a los datos de titulares de tarjetas o sistemas que almacenan, procesan o transmiten datos de titulares de tarjetas proporciona la oportunidad de que individuos no autorizados puedan acceder y/o retirar copias impresas que contengan datos de titulares de tarjetas; por lo tanto, el acceso físico debe restringirse adecuadamente.

Hay tres áreas diferentes mencionadas en el Requisito 9:

1. Los requisitos que se refieren específicamente a áreas sensibles están destinados a aplicarse solamente en esas áreas.
2. Los requisitos que se refieren específicamente al entorno de datos del titular de la tarjeta (CDE) están destinados a aplicarse a todo el CDE, incluida cualquier área sensible que resida dentro del CDE.
3. Los requisitos que se refieren específicamente a las instalaciones físicas hacen referencia a los tipos de controles que se pueden administrar de manera más amplia en el límite físico de un establecimiento comercial (como un edificio) dentro del cual residen los CDE y las áreas sensibles. Estos controles a menudo existen fuera de un CDE o un área sensible, por ejemplo, un puesto de guardia que identifica, acredita y registra a los visitantes. El término "instalación" se utiliza para reconocer que estos controles pueden existir en diferentes lugares dentro de una instalación física, por ejemplo, en la entrada del edificio o en una entrada interna a un centro de datos o espacio de oficinas.

Consulte el Anexo G para conocer las definiciones de "medios", "personal", "áreas sensibles" y otros términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
9.1 Se definen y comprenden los procesos y mecanismos para restringir el acceso físico a los datos del titular de la tarjeta.		
Requisitos del Enfoque Definido **9.1.1** Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 9 están: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la supervisión para el cumplimiento con las actividades dentro del Requisito 9 están definidas y se cumplen por parte de todo el personal involucrado. Todas las actividades de soporte son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.	**Procedimientos de Prueba del Enfoque Definido** **9.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 9 son administrados de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** El Requisito 9.1.1 trata sobre la gestión y el mantenimiento eficiente de las diversas políticas y procedimientos especificados en el Requisito 9. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 9, es igualmente importante garantizar que se documenten, se mantengan y se difundan adecuadamente. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocio. Por esta razón, considere actualizar estos documentos lo antes posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las políticas de seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma consistente y de acuerdo a los objetivos de la política. Las políticas y procedimientos, incluidas las actualizaciones, se comunican activamente a todo el personal involucrado y están respaldadas por procedimientos operativos que describen cómo realizar las actividades.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
9.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 9 están documentadas, asignadas y comprendidas.	**9.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y responsabilidades para realizar las actividades del Requisito 9 estén documentadas y asignadas.	Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que, por lo tanto, las actividades críticas no se realicen.
Objetivo del Enfoque Personalizado	**9.1.2.b** Entreviste al personal responsable de desarrollar las actividades del Requisito 9 para verificar que los roles y responsabilidades son asignados según están documentados y son comprendidos.	**Buenas Prácticas**
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 9. El personal es responsable del continuo y correcto funcionamiento de estos requisitos.		Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de la comunicación de los roles y responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de los roles y responsabilidades que les han sido asignados. Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).

Requisitos y Procedimientos de Prueba		Guía
9.2 Los controles de acceso físico gestionan la entrada a las instalaciones y sistemas que contengan datos de titulares de tarjeta.		
Requisitos del Enfoque Definido **9.2.1** Existen controles de entrada a las instalaciones apropiados para restringir el acceso físico a los sistemas en el CDE. **Objetivo del Enfoque Personalizado** Los componentes del sistema en el CDE no pueden ser accedidos físicamente por personal no autorizado.	**Procedimientos de Prueba del Enfoque Definido** **9.2.1** Observe los controles de entrada y entreviste al personal responsable para verificar que existen controles de seguridad física para restringir el acceso a los sistemas en el CDE.	**Objetivo** Sin controles de acceso físico, personas no autorizadas podrían potencialmente conseguir acceso al CDE e información sensible, o podrían alterar configuraciones de los sistemas, introducir vulnerabilidades en la red o destruir o robar equipos. Por lo tanto, el objetivo de este requisito es controlar el acceso físico al CDE a través de controles de seguridad física, tales como lectores de tarjetas de identificación u otros mecanismos como cerraduras y llaves. **Buenas Prácticas** Cualquiera que sea el mecanismo que cumpla con este requisito, debe ser suficiente para que la organización verifique que sólo se concede acceso al personal autorizado. **Ejemplos** Los controles de entrada a las instalaciones incluyen controles de seguridad física en cada sala de ordenadores, centro de datos y otras áreas físicas con sistemas en el CDE. Esto también puede incluir los lectores de tarjetas de identificación u otros dispositivos que gestionen los controles de acceso físico, tales como cerraduras y llaves con una lista actualizada de todos los individuos que tienen las llaves.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
9.2.1.1 El acceso físico individual a las áreas sensibles dentro del CDE se monitoriza con cámaras de video vigilancia o mecanismos de control de acceso físico (o ambos) como sigue: • Los puntos de entrada y salida hacia/desde las áreas sensibles dentro del CDE son monitorizados. • Los dispositivos o mecanismos de monitorización están protegidos contra la manipulación o la desactivación. • Los datos recogidos se revisan y se correlacionan con otras entradas. • Los datos recogidos se almacenan durante al menos tres meses, a menos que la ley lo restrinja.	**9.2.1.1.a** Observe los puntos de acceso físico de individuos a las áreas sensibles dentro del CDE para verificar que haya cámaras de video vigilancia o mecanismos de control de acceso físico (o ambos) para monitorizar los puntos de entrada y salida. **9.2.1.1.b** Observe los puntos de acceso físico de individuos a las áreas sensibles dentro del CDE para verificar que las cámaras de video vigilancia o mecanismos de control de acceso físico (o ambos) están protegidos contra la manipulación o desactivación. **9.2.1.1.c** Observe los mecanismos de control de acceso físico y/o las cámaras de video vigilancia y entreviste al personal responsable para verificar que: • Los datos recogidos por las cámaras de video vigilancia y/o los mecanismos de control de acceso físico se revisan y se correlacionan con otras entradas. • Los datos recogidos se almacenan durante al menos tres meses.	Mantener el detalle de las personas que entran y salen de las áreas sensibles puede ayudar en las investigaciones de violaciones físicas al identificar a las personas que accedieron físicamente a las áreas sensibles, así como el momento en que entraron y salieron. **Buenas Prácticas** Cualquiera que sea el mecanismo que cumpla con este requisito, debe monitorizar eficazmente todos los puntos de entrada y salida a áreas sensibles. Los delincuentes que intentan ingresar físicamente a las áreas sensibles, suelen intentar desactivar o eludir los controles de monitorización y vigilancia. Para proteger estos controles de la manipulación, las cámaras de video vigilancia podrían colocarse de forma que queden fuera del alcance y/o ser supervisadas para detectar la manipulación. Del mismo modo, los mecanismos de control de acceso físico podrían ser supervisados o tener protecciones físicas instaladas para evitar que sean dañados o desactivados por individuos malintencionados.
Objetivo del Enfoque Personalizado Se mantienen registros confiables y verificables de las entradas/salidas físicas de los individuos hacia/desde áreas sensibles.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **9.2.2** Se implementan controles físicos y/o lógicos para restringir el uso de tomas (o puertos) de red de acceso público dentro de la instalación. **Objetivo del Enfoque Personalizado** Los dispositivos no autorizados no pueden conectarse a la red de la entidad desde áreas públicas dentro de la instalación.	**Procedimientos de Prueba del Enfoque Definido** **9.2.2** Entreviste al personal responsable y observe las ubicaciones de la toma (o puertos) de red de acceso público para verificar que existen controles físicos y/o lógicos para restringir el acceso a la toma (o puertos) de red de acceso público dentro de la instalación.	**Objetivo** Restringir el acceso a las tomas de red (o puertos de red) evitará que personas malintencionadas se conecten a tomas de red fácilmente disponibles y obtengan acceso al CDE o a los sistemas conectados al CDE. **Buenas Prácticas** Tanto si se utilizan controles lógicos o físicos, o una combinación de ambos, estos deben impedir que una persona o un dispositivo que no esté explícitamente autorizado pueda conectarse a la red. **Ejemplos** Los métodos para cumplir con este requisito incluyen que las tomas de red situadas en áreas públicas y áreas accesibles por visitantes puedan ser deshabilitadas y sólo activadas cuando el acceso a la red esté explícitamente autorizado. Alternativamente, se podrían implementar procesos para asegurar que los visitantes son escoltados en todo momento en las áreas con tomas de red activas.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **9.2.3** El acceso físico a los puntos de acceso inalámbricos, puertas de enlace *(gateways),* hardware de redes y de comunicaciones y líneas de telecomunicaciones dentro de la instalación está restringido. **Objetivo del Enfoque Personalizado** El personal no autorizado no puede acceder al equipamiento físico de red.	**Procedimientos de Prueba del Enfoque Definido** **9.2.3** Entreviste al personal responsable y observe la ubicación del hardware y de las líneas para verificar que el acceso físico a los puntos de acceso inalámbrico, puertas de enlace (*gateway),* hardware de redes y de comunicaciones y líneas de telecomunicaciones dentro de la instalación está restringido.	**Objetivo** Sin la seguridad física apropiada en el acceso a los componentes y dispositivos inalámbricos, y al equipamiento y las líneas de redes y telecomunicaciones, usuarios malintencionados podrían obtener acceso a los recursos de la red de la entidad. Adicionalmente, podrían conectar sus propios dispositivos a la red para obtener acceso no autorizado al CDE o a sistemas conectados al CDE. Además, al proteger el hardware de redes y de comunicaciones se evita que usuarios malintencionados puedan interceptar el tráfico de la red o que conectar físicamente sus propios dispositivos a los recursos de la red cableada.
Requisitos del Enfoque Definido **9.2.4** El acceso a las consolas en áreas sensibles está restringido mediante bloqueo cuando no están en uso. **Objetivo del Enfoque Personalizado** Las consolas físicas dentro de áreas sensibles no pueden ser utilizadas por personal no autorizado.	**Procedimientos de Prueba del Enfoque Definido** **9.2.4** Observe el intento de un administrador del sistema de iniciar sesión en consolas en áreas sensibles y verifique que estén "bloqueadas" para evitar el uso no autorizado.	**Objetivo** El bloqueo de las pantallas de inicio de sesión de las consolas evita que personas no autorizadas accedan a información sensible, alteren las configuraciones del sistema, introduzcan vulnerabilidades en la red o destruyan registros.

Requisitos y Procedimientos de Prueba		Guía
9.3 Se autoriza y gestiona el acceso físico de personal y visitantes.		
Requisitos del Enfoque Definido **9.3.1** Se implementan procedimientos para autorizar y administrar el acceso físico del personal al CDE, que incluyen: • Identificación de personal. • Gestionar cambios en los requisitos de acceso físico de una persona. • Revocación o rescisión de la identificación del personal. • Limitar el acceso al proceso o sistema de identificación al personal autorizado. **Objetivo del Enfoque Personalizado** Los requisitos de acceso al CDE físico se definen y hacen cumplir para identificar y autorizar al personal.	**Procedimientos de Prueba del Enfoque Definido** **9.3.1.a** Evalúe los procedimientos documentados para verificar que los procedimientos para autorizar y administrar el acceso físico del personal al CDE estén definidos de acuerdo con todos los elementos especificados en este requisito. **9.3.1.b** Observe los métodos de identificación, tales como lasos los gafetes tarjetas de identificación, y los procesos para verificar que el personal en del CDE esté claramente identificado. **9.3.1.c** Observe que el acceso al proceso de identificación, como un sistema de gafetes, esté limitado al personal autorizado.	**Objetivo** El establecimiento de procedimientos para otorgar, administrar y eliminar el acceso cuando ya no es necesario, garantiza que se impida a personas no autorizadas ingresar a las áreas que contienen datos de titulares de tarjetas. Además, es importante limitar el acceso al sistema de gafetes y a los materiales de producción de credenciales reales para evitar que personal no autorizado haga sus propios gafetes y/o establezca sus propias reglas de acceso. **Buenas Prácticas** Es importante identificar visualmente al personal que está físicamente presente y determinar si el individuo es un visitante o un empleado. **Ejemplos** Una forma de identificar al personal es asignarle gafetes.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Controlar el acceso físico a las áreas sensibles ayuda a garantizar que solo se conceda acceso al personal autorizado con una necesidad legítima de negocios. **Buenas Prácticas** Siempre que sea posible, las organizaciones deben tener políticas y procedimientos para garantizar que antes de que el personal abandone la organización, todos los mecanismos de acceso físico sean devueltos o desactivados tan pronto como sea posible después de su partida. Esto asegurará que el personal no pueda ingresar físicamente a áreas sensibles una vez que finalice su empleo.
9.3.1.1 El acceso físico a áreas sensibles dentro del CDE para el personal se controla de la siguiente manera: • El acceso está autorizado y se basa en la función del trabajo individual. • El acceso se revoca inmediatamente después de la terminación. • Todos los mecanismos de acceso físico, como llaves, tarjetas de acceso, etc., se devuelven o desactivan al finalizar.	**9.3.1.1.a** Observe al personal en áreas sensibles dentro del CDE, entreviste al personal responsable y examine las listas de control de acceso físico para verificar que: • Se autoriza el acceso a la zona sensible. • Se requiere acceso físico para desempeñar la función laboral del individuo.	
	9.3.1.1.b Observe los procesos y entreviste al personal para verificar que el acceso de todo el personal se revoque inmediatamente después de la terminación.	
Objetivo del Enfoque Personalizado El personal no autorizado no puede ingresar a las áreas sensibles.	**9.3.1.1.c** En cuanto al personal que ya no labora en la entidad, revise las listas de controles de acceso físico y entreviste al personal responsable para verificar que todos los mecanismos de acceso físico (como llaves, tarjetas de acceso, etc.) fueron devueltos o desactivados.	

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
9.3.2 Se implementan procedimientos para autorizar y administrar el acceso de visitantes al CDE, que incluyen: • Los visitantes son autorizados antes de ingresar. • Los visitantes están acompañados en todo momento. • Los visitantes están claramente identificados y reciben un gafete u otra identificación con fecha de caducidad. • Los gafetes de visitante u otra identificación distinguen visiblemente a los visitantes del personal.	**9.3.2.a** Evalúe los procedimientos documentados y entreviste al personal para verificar que los procedimientos estén definidos para autorizar y administrar el acceso de visitantes al CDE de acuerdo con todos los elementos especificados en este requisito.	Los controles de visitantes son importantes para reducir la posibilidad de que personas no autorizadas y malintencionadas puedan ingresar a las instalaciones y, potencialmente, a los datos de los titulares de tarjetas. Los controles de visitas aseguran que estos sean identificables como visitas de manera que el personal pueda monitorear sus actividades y que su acceso esté restringido solo a la duración del tiempo legítimo de su visita.
	9.3.2.b Observe los procesos cuando los visitantes están presentes en el CDE y entreviste al personal para verificar que los visitantes: • Los visitantes están autorizados para ingresar al CDE. • Son escoltados en todo momento dentro del CDE.	
	9.3.2.c Observe el uso de gafetes de visitante u otra identificación para verificar que la credencial u otra identificación no permita el acceso sin escolta al CDE.	
	9.3.2.d Observe a los visitantes en el CDE para verificar que: • Todos los visitantes utilizan gafetes de visitante u otra identificación. • Los gafetes de visitante u otra identificación distinguen fácilmente a los visitantes del personal.	
Objetivo del Enfoque Personalizado	**9.3.2.e** Evalúe los gafetes de visitantes u otra identificación y observe la evidencia en el sistema de credenciales para verificar que los gafetes de visitantes u otras identificaciones tienen una fecha de caducidad.	
Los requisitos para el acceso de visitantes al CDE se definen y se hacen cumplir. Los visitantes no pueden exceder cualquier acceso físico autorizado permitido mientras están en el CDE.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **9.3.3** Los gafetes de visitante o la identificación se devuelven o desactivan antes de que los visitantes abandonen las instalaciones, o en su fecha de caducidad. **Objetivo del Enfoque Personalizado** Los gafetes o credenciales de visitante no se pueden reutilizar después de la fecha de caducidad.	**Procedimientos de Prueba del Enfoque Definido** **9.3.3** Observe a los visitantes que salen de la instalación y entreviste al personal para verificar que los gafetes de visitantes u otra identificación se devuelvan o se desactiven antes de que los visitantes abandonen las instalaciones o en la fecha de su caducidad.	**Objetivo** Asegurarse de que los gafetes de visitante se devuelvan o se desactiven al momento de caducidad o finalización de la visita evita que personas malintencionadas utilicen un pase previamente autorizado para obtener acceso físico al edificio una vez finalizada la visita.
Requisitos del Enfoque Definido **9.3.4** Se utiliza un registro de visitantes para mantener un registro físico de las actividades de los visitantes dentro de la instalación y dentro de las áreas sensibles, que incluye: • El nombre del visitante y la organización representada. • La fecha y hora de la visita. • El nombre del personal que autoriza el acceso físico. • Los datos recogidos se almacenan durante al menos tres meses, a menos que la ley lo restrinja. **Objetivo del Enfoque Personalizado** Se mantienen registros de acceso de visitantes que permiten la identificación de personas.	**Procedimientos de Prueba del Enfoque Definido** **9.3.4.a** Evalúe el registro de visitantes y entreviste al personal responsable para verificar que se utilice un registro de visitantes para registrar el acceso físico a las instalaciones y las áreas sensibles. **9.3.4.b** Evalúe el registro de visitantes y verificar que el registro contenga: • El nombre del visitante y la organización representada. • El nombre del personal que autoriza el acceso físico. • Fecha y hora de la visita. **9.3.4.c** Evalúe las ubicaciones de almacenamiento de registros de visitantes y entreviste al personal responsable para verificar que el registro se conserve durante al menos tres meses, a menos que la ley indique lo contrario.	**Objetivo** Un registro de visitantes que documente la información mínima sobre el visitante es fácil y económico de mantener. Ayudará a identificar el acceso físico histórico a un edificio o a una sala y el potencial acceso a los datos del titular de la tarjeta. **Buenas Prácticas** Cuando se registra la fecha y la hora de la visita, se considera una buena práctica incluir las horas de entrada y de salida, ya que proporcionan información de seguimiento útil y aseguran que todos los visitantes han abandonado el sitio al final del día. También es bueno verificar que las identificaciones de los visitantes (licencia de conducir, etc.) coincidan con el nombre que puso en el registro de visitantes.

Requisitos y Procedimientos de Prueba		Guía
9.4 Los medios con datos de titulares de tarjetas se almacenan, acceden, distribuyen y destruyen de forma segura.		
Requisitos del Enfoque Definido **9.4.1** Todos los medios que contienen datos de tarjetahabientes están protegidos físicamente. **Objetivo del Enfoque Personalizado** El personal no autorizado no puede acceder a los medios que contienen datos de tarjetahabientes.	**Procedimientos de Prueba del Enfoque Definido** **9.4.1.** Evalúe la documentación para verificar que los procedimientos definidos para proteger los datos de tarjetahabientes incluyen controles para asegurar físicamente todos los esos medios.	**Objetivo** Los controles para proteger físicamente los medios están destinados a evitar que personas no autorizadas obtengan acceso a los datos de titulares de tarjetas en cualquier formato. Los datos de titulares de tarjetas son susceptibles de ser visualizados, copiados o escaneos sin autorización si están desprotegidos mientras están en medios extraíbles o portátiles, impresos o dejados en el escritorio de alguien.
9.4.1.1 Las copias de seguridad sin conexión con los datos de titulares tarjetas se almacenan en una ubicación segura. **Objetivo del Enfoque Personalizado** El personal no autorizado no tendrá acceso a las copias de seguridad de datos fuera de línea.	**9.4.1.1.a** Evalúe la documentación para verificar que los procedimientos estén definidos a fin de proteger físicamente las copias de seguridad fuera de línea que contengan los datos de titulares de tarjetas en una ubicación segura. **9.4.1.1.b** Evalúe los registros u otra documentación y entreviste al personal responsable en la ubicación de almacenamiento para verificar que las copias de seguridad de datos fuera de línea, se guarden en una ubicación segura.	**Objetivo** Si se almacenan en una instalación no segura, las copias de seguridad que contienen los datos de titulares de tarjetas se pueden perder, ser robados o ser copiados fácilmente con fines maliciosos. **Buenas Prácticas** Para el almacenamiento seguro de los medios de apoyo, una buena práctica es almacenar los medios en una instalación fuera del sitio, como un sitio alternativo o de apoyo o una instalación de almacenamiento comercial.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** La realización de revisiones periódicas de las instalaciones de almacenamiento permite a la organización abordar los problemas de seguridad identificados con prontitud, minimizando riesgos potenciales. Es importante que la entidad esté consciente de la protección del área donde se almacenan los datos.
9.4.1.2 La protección de las ubicaciones de las copias de seguridad fuera de línea que contienen los datos de titulares de tarjetas, se revisa al menos una vez cada 12 meses.	**9.4.1.2.a** Evalúe la documentación para verificar que los procedimientos estén definidos para revisar la seguridad de las ubicaciones de apoyos fuera de línea que contengan datos de titulares de tarjetas al menos una vez cada 12 meses.	
	9.4.1.2.b Evalúe los procedimientos documentados, los registros u otra documentación, y entreviste al personal responsable en las ubicaciones de almacenamiento para verificar que la seguridad de la ubicación de almacenamiento se revise al menos una vez cada 12 meses.	
Objetivo del Enfoque Personalizado		
Los controles de seguridad que protegen las copias de seguridad fuera de línea se verifican periódicamente mediante inspección.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Los datos no señalados como confidenciales pueden no estar adecuadamente protegidos o pueden perderse o ser robados. **Buenas Prácticas** Es importante que los datos se identifiquen de manera que su estado de clasificación sea evidente. Sin embargo, esto no significa que los datos necesiten llevar una etiqueta de "confidencial".
9.4.2 Todos los datos de titulares de tarjetas se clasifican de acuerdo con la confidencialidad de esos datos.	**9.4.2.a** Evalúe la documentación para verificar que los procedimientos estén definidos para clasificar los datos de titulares de tarjetas de acuerdo con el nivel de confidencialidad de esos datos.	
	9.4.2.b Evalúe los registros de medios u otra documentación para verificar que todos los datos estén clasificados de acuerdo con su nivel de confidencialidad.	
Objetivo del Enfoque Personalizado		
Los datos se clasifican y protegen adecuadamente.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **9.4.3** Los apoyos con datos de titulares de tarjetas enviados fuera de las instalaciones se protegen de la siguiente manera: • Los datos enviados fuera de las instalaciones se registran. • Los datos se envían por mensajería segura u otro método de entrega que pueda ser rastreado con precisión. • Los registros de seguimiento fuera de las instalaciones incluyen detalles sobre la ubicación de los datos. **Objetivo del Enfoque Personalizado** Los datos se aseguran y se rastrean cuando se transportan fuera de las instalaciones.	**Procedimientos de Prueba del Enfoque Definido** **9.4.3.a** Evalúe la documentación para verificar que los procedimientos están definidos a fin de asegurar los datos enviados fuera de la instalación de acuerdo con todos los elementos especificados en este requisito. **9.4.3.b** Entreviste al personal y examine los registros para verificar que todos los datos enviados fuera de la instalación se registran y se envían a través de un servicio de mensajería seguro u otro método de entrega que pueda rastrearse. **9.4.3.c** Evalúe los registros de seguimiento de todos los datos enviados fuera de las instalaciones para verificar que los detalles de seguimiento estén documentados.	**Objetivo** Los apoyos pueden perderse o ser robados si se envían a través de un método no rastreable, como el correo postal ordinario. El uso de mensajería segura para entregar cualquier medio que contenga datos de titulares de tarjetas permite a las organizaciones utilizar sus sistemas de seguimiento para mantener el inventario y la ubicación de los envíos.
Requisitos del Enfoque Definido **9.4.4** La gerencia aprueba todos los movimientos de apoyos con datos de titulares de tarjetas que se trasladan fuera de las instalaciones (incluso cuando son distribuidos a particulares). **Objetivo del Enfoque Personalizado** Los apoyos no pueden salir de una instalación sin la aprobación del personal responsable.	**Procedimientos de Prueba del Enfoque Definido** **9.4.4.a** Evalúe la documentación para verificar se han definido los procedimientos para garantizar que los apoyos que se trasladan fuera de las instalaciones son aprobados por la gerencia. **9.4.4.b** Evalúe los registros de seguimiento de los apoyos fuera de las instalaciones y entreviste al personal responsable para verificar que se obtiene la autorización apropiada de parte de la gerencia, *(continúa en la página siguiente)*	**Objetivo** Sin un proceso sólido que garantice la aprobación de todos los movimientos de datos antes de que sean retirados de zonas seguras, estos no podrían ser rastreados ni protegidos adecuadamente, y su ubicación sería desconocida, lo que llevaría a su robo o pérdida.

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Las personas que aprueban los movimientos de los apoyos deben tener el nivel adecuado de autoridad de gestión para conceder esta aprobación. Sin embargo, no se requiere específicamente que dichas personas tengan el título de "gerente".	para todos los apoyos trasladados fuera de las instalaciones (incluidos los apoyos distribuidos a particulares).	
Requisitos del Enfoque Definido **9.4.5** Se mantienen registros de inventario de todos los apoyos electrónicos con datos de titulares de tarjetas. **Objetivo del Enfoque Personalizado** Se mantienen inventarios precisos de los apoyos electrónicos almacenados.	**Procedimientos de Prueba del Enfoque Definido** **9.4.5.a** Evalúe la documentación para verificar que se definen los procedimientos para mantener los registros de inventario de los apoyos electrónicos. **9.4.5.b** Evalúe los registros de inventario de apoyos electrónicos y entreviste al personal responsable para verificar que se mantengan los registros.	**Objetivo** Sin los métodos de inventario y controles de almacenamiento apropiados, los apoyos electrónicos robados o perdidos podrían pasar desapercibidos durante un tiempo indefinido.
Requisitos del Enfoque Definido **9.4.5.1** Los inventarios de apoyos electrónicos con datos de titulares de tarjetas se realizan al menos una vez cada 12 meses. **Objetivo del Enfoque Personalizado** Los inventarios de datos se verifican periódicamente.	**Procedimientos de Prueba del Enfoque Definido** **9.4.5.1.a** Evalúe la documentación para verificar que se han definido procedimientos para realizar inventarios de los apoyos electrónicos con datos de titulares de tarjetas al menos una vez cada 12 meses. **9.4.5.1.b** Evalúe los inventarios de registros electrónicos de datos y entreviste al personal para verificar que se realicen al menos una vez cada 12 meses.	**Objetivo** Sin los métodos de inventario y controles de almacenamiento apropiados, los apoyos electrónicos robados o perdidos podrían pasar desapercibidos durante un tiempo indefinido.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
9.4.6 Los materiales impresos con datos de titulares de tarjetas se destruyen cuando ya no se necesitan por razones de negocios o legales, de la siguiente manera: • Los materiales se trituran transversalmente, se incineran o se pulverizan de forma que los datos de los titulares de tarjetas no puedan reconstruirse. • Los materiales se guardan en contenedores de almacenamiento seguro antes de su destrucción.	**9.4.6.a** Evalúe la política de destrucción periódica de materiales impresos para comprobar que se han definido procedimientos para destruir los materiales impresos con datos de los titulares de las tarjetas cuando ya no se necesiten por motivos de negocio o legales, de acuerdo con todos los elementos especificados en este requisito.	Si no se toman medidas para destruir la información que contienen los materiales impresos antes de su eliminación, personas malintencionadas pueden recuperar la información de los materiales desechados, lo que puede poner en peligro los datos. Por ejemplo, personas malintencionadas pueden utilizar una técnica conocida como "búsqueda en el contenedor", en la que buscan en los cubos de basura y en los basureros de reciclaje, materiales impresos con información que puedan utilizar para lanzar un ataque. Proteger los contenedores de almacenamiento utilizados para el material que será destruido evita que información confidencial sea capturada durante la recolección de esos materiales.
	9.4.6.b Observe los procesos y entreviste al personal para verificar que los materiales impresos se trituran, incineran o pulverizan de manera que los datos de titulares de tarjetas no puedan reconstruirse.	**Buenas Prácticas** Considere la posibilidad de que los contenedores que contienen material que será destruido tengan algún candado que impida el acceso a su contenido, o que impida físicamente el acceso al interior del contenedor.
Objetivo del Enfoque Personalizado Los datos del titular de la tarjeta no pueden recuperarse de los materiales impresos que han sido destruidos o que están pendientes de destrucción.	**9.4.6.c** Observe los contenedores de almacenamiento utilizados para los materiales que contienen información que debe ser destruida a fin de verificar que sean seguros.	**Información Adicional** *Refiérase a Publicación Especial NIST 800-88, Revisión 1: Pautas para el Saneamiento de Medios.*
Notas de Aplicabilidad Estos requisitos relativos a la destrucción de materiales impresos cuando éstos ya no son necesarios por motivos de negocio o legales son independientes y distintos del requisito 3.2.1 PCI DSS, que se refiere a la eliminación segura de los datos de los titulares de tarjetas cuando ya no son necesarios de acuerdo con las políticas de retención de datos de los titulares de tarjetas de la entidad.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **9.4.7** Los medios de almacenamiento electrónicos con datos de titulares de la tarjeta se destruyen cuando ya no se necesitan por razones de negocio o legales mediante una de las siguientes opciones: • El medio de almacenamiento electrónico se destruye. • Los datos de titulares de tarjetas se vuelven irrecuperables, de modo que no pueden reconstruirse. **Objetivo del Enfoque Personalizado** Los datos de titulares de las tarjetas no pueden recuperarse de los medios de almacenamiento que han sido borrados o destruidos. **Notas de Aplicabilidad** Estos requisitos relativos a la destrucción de medios de almacenamiento cuando éstos ya no son necesarios por motivos de negocio o legales son independientes y distintos del requisito 3.2.1 PCI DSS, que se refiere a la eliminación segura de los datos de los titulares de tarjetas cuando ya no son necesarios de acuerdo con las políticas de retención de datos de los titulares de tarjetas de la entidad.	**Procedimientos de Prueba del Enfoque Definido** **9.4.7.a** Evalúe la política de destrucción periódica de medios de almacenamiento para comprobar que se definen procedimientos para destruir los medios de almacenamiento electrónicos cuando ya no se necesiten por razones de negocio o legales de acuerdo con todos los elementos especificados en este requisito. **9.4.7.b** Observe el proceso de destrucción de medios de almacenamiento y entreviste al personal responsable para verificar que los medios de almacenamiento electrónicos con datos de titulares de tarjetas se destruyen mediante uno de los métodos especificados en este requisito.	**Objetivo** Si no se adoptan medidas para destruir la información contenida en los medios de almacenamiento electrónicos cuando ya no se necesiten, personas malintencionadas pueden recuperar información de los medios de almacenamiento desechados, lo que puede poner en peligro los datos. Por ejemplo, individuos malintencionados pueden utilizar una técnica conocida como "búsqueda en el contenedor", en la que buscan en los cubos de basura y en los contenedores de reciclaje información que puedan utilizar para lanzar un ataque. **Buenas Prácticas** La función de eliminación en la mayoría de los sistemas operativos permite recuperar los datos eliminados, por lo que, en su lugar, se debe utilizar una función de eliminación segura o una aplicación para que los datos sean irrecuperables. **Ejemplos** Los métodos para destruir de forma segura los medios de almacenamiento electrónicos incluyen el borrado seguro de acuerdo con los estándares aceptados por la industria para borrado seguro, la des-magnetización o la destrucción física (como la trituración de los discos duros). **Información Adicional** *Refiérase a la Publicación Especial NIST 800-88, Revisión 1: Pautas para el Saneamiento de Medios.*

Requisitos y Procedimientos de Prueba		Guía
9.5 Los dispositivos de Punto de Interacción (POI) están protegidos contra manipulaciones y sustituciones no autorizadas.		
Requisitos del Enfoque Definido **9.5.1** Los dispositivos POI que capturan los datos de las tarjetas de pago a través de la interacción física directa con el factor de forma de la tarjeta de pago están protegidos contra la manipulación y la sustitución no autorizada, incluyendo lo siguiente: • Mantener una lista de dispositivos de POI. • Inspeccionar periódicamente los dispositivos POI en busca de manipulaciones o sustituciones no autorizadas. • Formar al personal para que esté atento a los comportamientos sospechosos y denuncie las manipulaciones o sustituciones no autorizadas de los dispositivos. **Objetivo del Enfoque Personalizado** La entidad ha definido procedimientos para proteger y gestionar los dispositivos de los puntos de interacción. Las expectativas, los controles y la supervisión para la gestión y la protección de los POI están definidos y son respetados por el personal afectado. *(continúa en la página siguiente)*	**Procedimientos de Prueba del Enfoque Definido** **9.5.1** Evalúe las políticas y procedimientos documentados para verificar que los procesos estén definidos e incluyan todos los elementos especificados en este requisito.	**Objetivo** Los delincuentes intentan robar los datos de tarjetas de pago robando y/o manipulando los dispositivos y terminales de lectura de tarjetas. Los delincuentes intentan robar los dispositivos para aprender a entrar en ellos, y a menudo intentan sustituir los dispositivos legítimos por dispositivos fraudulentos que les envían los datos de las tarjetas de pago cada vez que se introduce una tarjeta. También intentan añadir componentes de "*skimming"* en el exterior de los dispositivos, diseñados para capturar los datos de las tarjetas de pago antes de que entren en el dispositivo; por ejemplo, colocando un lector de tarjetas adicional sobre el lector de tarjetas legítimo, de modo que los datos de las tarjetas de pago sean capturados dos veces: una por el componente del delincuente y otra por el componente legítimo del dispositivo. De este modo, las transacciones pueden seguir completándose sin interrupción mientras el delincuente "roba" los datos de la tarjeta de pago durante el proceso. **Información Adicional** En el sitio web PCI SCC se pueden encontrar más prácticas recomendadas sobre la prevención del "*skimming".*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Estos requisitos se aplican a los dispositivos de POI desplegados que se utilizan en transacciones con tarjeta física (es decir, un factor de forma de tarjeta de pago como una tarjeta que se pasa, se toca o se introduce). Este requisito no está destinado a aplicarse a los componentes manuales de introducción de claves PAN, como los teclados de ordenador. Este requisito es recomendado, pero no exigible, para los componentes manuales de introducción de claves PAN, como los teclados de ordenador. Este requisito no se aplica a los dispositivos comerciales listos para usar (COTS) (por ejemplo, teléfonos inteligentes o tabletas), que son dispositivos móviles propiedad de comerciantes, diseñados para su distribución en el mercado masivo.		
Requisitos del Enfoque Definido **9.5.1.1** Se mantiene una lista actualizada de los dispositivos POI, que incluye: • Marca y modelo del dispositivo. • Ubicación del dispositivo. • Número de serie del dispositivo u otros métodos de identificación única. **Objetivo del Enfoque Personalizado** La identidad y la ubicación de los dispositivos POI se registran y se conoce en todo momento.	**Procedimientos de Prueba del Enfoque Definido** **9.5.1.1.a** Evalúe la lista de dispositivos de POI para verificar que incluye todos los elementos especificados en este requisito. **9.5.1.1.b** Observe dispositivos POI y sus ubicaciones y compararlos con la lista para verificar que la lista es precisa y está actualizada. **9.5.1.1.c** Entreviste al personal para verificar que la lista de dispositivos POI se actualiza cuando se añaden, trasladan o retiran dispositivos, etc.	**Objetivo** Mantener una lista actualizada de los dispositivos POI contribuye a que la organización pueda rastrear el sitio donde se supone que están los dispositivos y a identificar rápidamente si falta un dispositivo o se pierde. **Buenas Prácticas** El método para mantener una lista de dispositivos puede ser automatizado (por ejemplo, un sistema de gestión de dispositivos) o manual (por ejemplo, documentado en registros electrónicos o en papel). En el caso de los dispositivos en movimiento, la ubicación puede incluir el nombre del personal al que se asigna el dispositivo. **Ejemplos** Los métodos para mantener la ubicación de los dispositivos incluyen la identificación de la dirección del sitio o instalación donde se encuentra el dispositivo.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoques Definido.**	
9.5.1.2 Las superficies de los dispositivos POI se inspeccionan periódicamente para detectar manipulaciones y sustituciones no autorizadas.	**9.5.1.2.a** Evalúe los procedimientos documentados para verificar que se han definido los procesos para las inspecciones periódicas de las superficies de los dispositivos POI a fin de detectar manipulaciones y sustituciones no autorizadas.	**Objetivo** Las inspecciones regulares de los dispositivos ayudarán a las organizaciones a detectar más rápidamente las manipulaciones a través de evidencias externas -por ejemplo, la adición de un *skimmer* o lector de tarjeta- o la sustitución de un dispositivo, minimizando así el impacto potencial del uso de dispositivos fraudulentos. **Buenas Prácticas** Los métodos de inspección periódica incluyen la comprobación del número de serie u otras características del dispositivo y la comparación de la información con la lista de dispositivos POI para verificar que el dispositivo no ha sido intercambiado con un dispositivo fraudulento. **Ejemplos** El tipo de inspección dependerá del dispositivo. Por ejemplo, se pueden utilizar fotografías de dispositivos que se sabe que son seguros para comparar el aspecto actual de un dispositivo con su aspecto original y ver si ha cambiado. Otra opción puede ser utilizar un rotulador seguro, como un rotulador de luz ultravioleta, para marcar las superficies y las aberturas de los dispositivos, de modo que cualquier manipulación o sustitución sea evidente. Los delincuentes suelen sustituir la cubierta exterior de un dispositivo para ocultar su manipulación, y estos métodos pueden ayudar a detectar esas actividades. Los proveedores de dispositivos también pueden proporcionar orientación sobre seguridad y guías de "cómo hacerlo" para ayudar a determinar si el dispositivo ha sido objeto de manipulación. *(continúa en la página siguiente)*
	9.5.1.2.b Entreviste al personal responsable y observe los procesos de inspección para verificar: • El personal conoce los procedimientos de inspección de los dispositivos. • Todos los dispositivos se inspeccionan periódicamente para detectar evidencias de manipulación y sustitución no autorizada.	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Los Dispositivos de Punto de Interacción no pueden ser manipulados, sustituidos sin autorización, ni se les pude instalar accesorios para *skimming* sin ser detectados a tiempo.		Los signos de que un dispositivo puede haber sido manipulado o sustituido incluyen: • Accesorios inapropiados conectados al dispositivo. • Etiquetas de seguridad que faltan o han sido reemplazadas. • Cubiertas rotas o de otro color. • Cambios en el número de serie u otras marcas externas.
Requisitos del Enfoque Definido **9.5.1.2.1** La frecuencia de las inspecciones a los dispositivos POI y el tipo de inspección que se realice se define en el análisis de riesgos específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1. **Objetivo del Enfoque Personalizado** Los dispositivos POI se inspeccionan con una frecuencia que se ajusta al riesgo de la entidad. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba del Enfoque Definido** **9.5.1.2.1.a** Evalúe el análisis de riesgos específico de la entidad en cuanto a la frecuencia de las inspecciones de dispositivos POI y el tipo de inspección realizada de acuerdo con todos los elementos especificados en el Requisito 12.3.1. **9.5.1.2.1.b** Evalúe los resultados documentados de las inspecciones de dispositivos y entreviste al personal para verificar si la frecuencia y tipo de inspección de realizada en los dispositivos POI están de acuerdo con el análisis de riesgo específico de la entidad para este requisito.	**Objetivo** Las entidades son las más indicadas para determinar la frecuencia de las inspecciones de los dispositivos POI en función del entorno en el que operan. **Buenas Prácticas** La frecuencia de las inspecciones dependerá de factores como la ubicación de un dispositivo y si éste está supervisado o no. Por ejemplo, los dispositivos que se dejan en áreas públicas sin supervisión del personal de la organización podrían ser inspeccionados más frecuentemente que los dispositivos que se mantienen en áreas seguras o supervisadas cuando son accesibles al público. Además, muchos proveedores de POI incluyen guías del usuario que indican la frecuencia con la que debe revisarse los dispositivos POI y con qué propósito - las entidades deben consultar la documentación de sus proveedores e incorporar esas recomendaciones en sus inspecciones periódicas.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoques Definidos**	**Objetivo**
9.5.1.3 Se proporciona capacitación para que el personal en entornos POI esté al tanto de los intentos de manipulación o reemplazo de dispositivos POI, lo que incluye: • Verificar la identidad de cualquier tercero que afirme ser personal de reparación o mantenimiento, antes de otorgarles acceso para modificar o solucionar problemas en los dispositivos. • Procedimientos para garantizar que los dispositivos no se instalen, reemplacen o devuelvan sin verificación. • Ser consciente de comportamientos sospechosos alrededor de los dispositivos. • Informar sobre comportamientos sospechosos e indicaciones de manipulación o sustitución de dispositivos al personal apropiado.	**9.5.1.3.a** Evalúe los materiales de capacitación para el personal en entornos de POI para verificar que incluyan todos los elementos especificados en este requisito. **9.5.1.3.b** Entreviste al personal en entornos de POI para verificar que hayan recibido capacitación y conozcan los procedimientos para todos los elementos especificados en este requisito.	Los delincuentes a menudo se hacen pasar por personal de mantenimiento autorizado para obtener acceso a los dispositivos POI. **Buenas Prácticas** La capacitación del personal debe incluir estar alerta e interrogar a cualquier persona que se presente para realizar el mantenimiento de los POI para asegurarse de que esté autorizado y tenga una orden de trabajo válida, incluidos los agentes, el personal de mantenimiento o reparación, los técnicos, los proveedores de servicio u otros terceros. Todos los proveedores que soliciten acceso a los dispositivos siempre deben ser verificados antes de que se les proporcione el acceso, por ejemplo, verificando con la administración o llamando a la compañía de mantenimiento de los POI, como el proveedor o adquirente, para verificación. Muchos delincuentes intentarán engañar al personal vistiéndose para el papel (por ejemplo, llevando cajas de herramientas y vestidos con ropa de trabajo), y también podrían estar informados sobre la ubicación de los dispositivos, por lo que el personal debe estar capacitado para seguir siempre los procedimientos. Otro truco que utilizan los delincuentes es enviar un dispositivo POI "nuevo" con instrucciones para cambiarlo por un dispositivo legítimo y "devolver" el dispositivo legítimo. Los delincuentes incluso pueden proporcionar franqueo de devolución a su dirección. Por lo tanto, el personal siempre debe verificar con su gerente o proveedor que el dispositivo es legítimo y proviene de una fuente confiable antes de instalarlo o usarlo para negocios. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado		
El personal está bien informado sobre los tipos de ataques contra dispositivos POI, las contramedidas técnicas y de procedimientos de la entidad, y pueden recibir asistencia y orientación siempre que sea necesario.		

Requisitos y Procedimientos de Prueba		Guía
		Ejemplos El comportamiento sospechoso que el personal debe conocer incluye intentos de personas desconocidas de desenchufar o abrir dispositivos. Asegurarse de que el personal conozca los mecanismos para denunciar comportamientos sospechosos y a quién denunciar dichos comportamientos (por ejemplo, un gerente o un oficial de seguridad) ayudará a reducir la probabilidad y el impacto potencial de que un dispositivo sea manipulado o sustituido.

Monitorear y Verificar las Redes Regularmente

Requisito 10: Registrar y Supervisar Todos los Accesos a los Componentes del Sistema y a los Datos de Tarjetahabientes

Secciones	
10.1	Se definen y documentan los procesos y mecanismos para ingresar y monitorear todos los accesos a los componentes del sistema y a los datos de titulares de tarjetas.
10.2	Los registros de auditoría se implementan para respaldar la detección de anomalías y actividades sospechosas, y el análisis forense de eventos.
10.3	Los registros de auditoría están protegidos contra la destrucción y las modificaciones no autorizadas.
10.4	Los registros de auditoría se revisan para identificar anomalías o actividades sospechosas.
10.5	El historial del registro de auditoría se conserva y está disponible para su análisis.
10.6	Los mecanismos de sincronización de la hora admiten una configuración de hora coherente en todos los sistemas.
10.7	Las fallas de los sistemas críticos de control de seguridad se detectan, se reportan y se responden de manera oportuna.

Descripción

Los mecanismos de registro y la capacidad de rastrear las actividades del usuario son fundamentales para evitar, detectar o minimizar el impacto de datos comprometidos. La existencia de registros en todos los componentes del sistema y del entorno de datos de titulares de tarjetas (CDE) permite el seguimiento, alertas y análisis cuando algo sale mal. Determinar la causa de una situación comprometida es difícil, si no imposible, sin los registros de actividad del sistema.

Este requisito se aplica a las actividades de los usuarios, incluidas las realizadas por empleados, contratistas, consultores y proveedores internos y externos, y otros terceros (por ejemplo, aquellos que brindan servicios de apoyo o mantenimiento).

Estos requisitos no aplican para los consumidores (titulares de tarjetas).

Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
10.1 Se definen y documentan los procesos y mecanismos para ingresar y monitorear todos los accesos a los componentes del sistema y a los datos de titulares de tarjetas.		
Requisitos del Enfoque Definido.	**Procedimientos de Prueba del Enfoques Definido.**	**Objetivo** El Requisito 10.1.1 trata sobre la gestión y mantención eficiente de las diversas políticas y procedimientos especificados en el Requisito 10. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 10, es igualmente importante garantizar que se documenten, se mantengan y se difundan adecuadamente. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocios. Por esta razón, considere actualizar estos documentos lo más pronto posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.
10.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 10 están: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.	**10.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos identificados en el Requisito 10 son administrados de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado		
Las expectativas, los controles y la vigilancia en el cumplimiento con las actividades dentro del Requisito 10 están definidos y cumplidos por el personal afectado. Todas las actividades de apoyo son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido.**	**Objetivo** Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que las actividades críticas no ocurran. **Buenas Prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
10.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 10 están documentadas, asignadas y comprendidas.	**10.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y responsabilidades para realizar las actividades del Requisito 10 estén documentadas y asignadas.	
	10.1.2.b Entreviste al personal responsable de desarrollar las actividades del Requisito 10 para verificar que los roles y responsabilidades se asignen según sean documentadas y entendidas.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 10. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
10.2 Los registros de auditoría se implementan para respaldar la detección de anomalías y actividades sospechosas, y el análisis forense de eventos.		
Requisitos del Enfoque Definido **10.2.1** Los registros de auditoría están habilitados y activos para todos los componentes del sistema y los datos de titulares de tarjetas. **Objetivo del Enfoque Personalizado** Se capturan registros de todas las actividades que afectan los componentes del sistema y los datos de titulares de tarjetas.	**Procedimientos de Prueba del Enfoque Definido** **10.2.1** Entreviste al administrador del sistema y examine las configuraciones del sistema para verificar que los registros de auditoría estén habilitados y activos para todos los componentes del sistema.	**Objetivo** El registro debe realizarse para todos los componentes del sistema. Los registros de auditoría envían alertas al administrador del sistema, proporcionan datos a otros mecanismos de supervisión, como los sistemas de detección de intrusiones (IDS) y las herramientas de sistemas de supervisión de eventos e información de seguridad (SIEM), y proporcionan al cliente un historial para la investigación posterior. El registro y análisis de eventos relevantes en materia de seguridad, permite a la organización identificar y rastrear actividades potencialmente maliciosas. **Buenas Prácticas** Cuando una entidad considera qué información guardar en sus registros, es importante recordar que la información almacenada en los registros de auditoría es confidencial y debe protegerse según los requisitos de este estándar. Se debe tener el cuidado de almacenar solo información esencial para minimizar riesgos.
Requisitos del Enfoque Definido **10.2.1.1** Los registros de auditoría capturan todo el acceso de los usuarios individuales a los datos de titulares de tarjetas. **Objetivo del Enfoque Personalizado** Se capturan registros de todo acceso de usuarios individuales a los datos de titulares de tarjetas.	**Procedimientos de Prueba del Enfoque Definido** **10.2.1.1** Evalúe las configuraciones del registro de auditoría y los datos de registro para verificar que se registre el acceso de todos los usuarios individuales a los datos de titulares de tarjetas.	**Objetivo** Es esencial tener un proceso o sistema que vincule el acceso de los usuarios a los componentes del sistema y a qué componentes han ingresado. Personas malintencionadas podrían obtener conocimiento de una cuenta de usuario con acceso a sistemas en el CDE, o podrían crear una nueva cuenta no autorizada para ingresar a los datos de titulares de tarjetas. **Buenas Prácticas** Un registro de todos los accesos individuales a los datos de titulares de tarjetas puede identificar qué cuentas pueden haber sido comprometidas o mal utilizadas.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **10.2.1.2** Los registros de auditoría almacenan todas las acciones realizadas por cualquier individuo con acceso administrativo, incluyendo cualquier uso interactivo de la aplicación o cuentas del sistema. **Objetivo del Enfoque Personalizado** Se capturan registros de todas las acciones realizadas por personas con privilegios elevados.	**Procedimientos de Prueba del Enfoque Definido** **10.2.1.2** Evalúe las configuraciones del registro de auditoría y los datos del registro para verificar que se registren todas las acciones realizadas por cualquier persona con acceso administrativo, incluyendo cualquier uso interactivo de la aplicación o las cuentas del sistema.	**Objetivo** Las cuentas con mayores privilegios de acceso, tales como la cuenta de "administrador" o "root", tienen el potencial de afectar significativamente la seguridad o la funcionalidad operativa de un sistema. Sin un registro de las actividades realizadas, la organización no puede rastrear ningún problema generado por un error administrativo, o por el uso indebido de privilegios hasta la acción y la cuenta específica que generó el problema. **Definiciones** Las cuentas con acceso administrativo son aquellas asignadas con privilegios o capacidades específicas para administrar sistemas, redes y / o aplicaciones. Las funciones o actividades consideradas administrativas van más allá de las realizadas por los usuarios habituales como parte de las funciones de negocios de rutina.
Requisitos del Enfoque Definido **10.2.1.3** Los registros de auditoría capturan todo el acceso a los mismos. **Objetivo del Enfoque Personalizado** Se capturan registros de todo el acceso a los registros de auditoría.	**Procedimientos de Prueba del Enfoque Definido** **10.2.1.3** Evalúe las configuraciones del registro de auditoría y los datos de registro para verificar que se capture el acceso a todos los registros de auditoría.	**Objetivo** Usuarios malintencionados a menudo intentan alterar los registros de auditoría para ocultar sus acciones. El registro de acceso permite a una organización rastrear cualquier inconsistencia o posible alteración de los registros a una cuenta individual. Tener registros que identifiquen cambios, adiciones y eliminaciones en los registros de auditoría puede ayudar a rastrear los pasos realizados por personal no autorizado.
Requisitos del Enfoque Definido **10.2.1.4** Los registros de auditoría capturan todos los intentos de acceso lógico inválidos. *(continúa en la página siguiente)*	**Procedimientos de Prueba del Enfoque Definido** **10.2.1.4** Evalúe las configuraciones del registro de auditoría y los datos del registro para verificar que se capturen los intentos de acceso lógico inválidos.	**Objetivo** Personas malintencionadas a menudo realizarán múltiples intentos de acceso a sistemas específicos. Los múltiples intentos de inicio de sesión inválidos pueden indicar intentos de "fuerza bruta" o de adivinación de una contraseña de un usuario no autorizado.

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Se capturan registros de todos los intentos de acceso inválidos.		
Requisitos del Enfoque Definido **10.2.1.5** Los registros de auditoría capturan todos los cambios en la identificación y credenciales de autenticación, lo que incluye, entre otros: • Creación de nuevas cuentas. • Elevación de privilegios. • Todos los cambios, adiciones o eliminaciones de cuentas con acceso administrativo.	**Procedimientos de Prueba del Enfoque Definido** **10.2.1.5** Evalúe las configuraciones del registro de auditoría y los datos del registro para verificar que los cambios en las credenciales de identificación y autenticación se registran de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** El registro de cambios en las credenciales de autenticación (incluyendo la elevación de privilegios, adiciones y eliminaciones de cuentas con acceso administrativo) proporciona evidencia residual de las actividades. Usuarios malintencionados pueden intentar manipular las credenciales de autenticación para eludirlas o hacerse pasar por una cuenta válida.
Objetivo del Enfoque Personalizado Se capturan registros de todos los cambios de identificación y credenciales de autenticación.		
Requisitos del Enfoque Definido **10.2.1.6** Los registros de auditoría capturan lo siguiente: • Toda inicialización de nuevos registros de auditoría y • Todo inicio, la detención o la pausa de los registros de auditoría existentes.	**Procedimientos de Prueba del Enfoque Definido** **10.2.1.6** Evalúe las configuraciones del registro de auditoría y los datos del registro para verificar que se capturan todos los elementos especificados en este requisito.	**Objetivo** Una práctica común de usuarios malintencionados para evitar ser detectados es apagar o pausar los registros de auditoría antes de realizar actividades ilícitas. La inicialización de los registros de auditoría podría indicar que un usuario deshabilitó la función de registro para ocultar sus acciones.
Objetivo del Enfoque Personalizado Se capturan registros de todos los cambios en el estado de actividad del registro de auditoría.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** El software malintencionado, como el malware,a menudo crea o reemplaza objetos a nivel del sistema de destino para controlar una función u operación en particular dentro de ese sistema. Al registrar cuando se crean o eliminan objetos a nivel del sistema, hará más fácil determinar si tales modificaciones fueron autorizadas.
10.2.1.7 Los registros de auditoría capturan toda la creación y eliminación de objetos a nivel del sistema.	**10.2.1.7** Evalúe las configuraciones del registro de auditoría y los datos del registro para verificar que se capture la creación y eliminación de objetos a nivel del sistema.	
Objetivo del Enfoque Personalizado		
Se capturan los registros de alteraciones que indican que un sistema ha sido modificado con respecto a su funcionalidad original.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Al registrar estos detalles para los eventos auditables en 10.2.1.1 hasta 10.2.1.7, se puede identificar rápidamente una falla de seguridad potencial con suficientes detalles para facilitar el seguimiento de actividades sospechosas.
10.2.2 Los registros de auditoría guardan los siguientes detalles para cada evento auditable: • Identificación del usuario. • Tipo de evento. • Fecha y hora. • Indicación de Exitoso o Fallido. • Origen del evento. • Identidad o nombre de los datos, componentes del sistema, recursos o servicios afectados (por ejemplo, nombre y protocolo).	**10.2.2** Entreviste al personal y examine las configuraciones del registro de auditoría para verificar que todos los elementos especificados en este requisito estén incluidos en las entradas del registro para cada evento auditable (desde 10.2.1.1 hasta 10.2.1.7).	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Se registran suficientes datos para poder identificar los intentos exitosos y fallidos y quién, qué, cuándo, dónde y cómo para cada evento enumerado en el requisito 10.2.1.		

Requisitos y Procedimientos de Prueba		Guía
10.3 Los registros de auditoría están protegidos contra la destrucción y las modificaciones no autorizadas.		
Requisitos del Enfoque Definido **10.3.1** El acceso de lectura a los archivos de registros de auditoría está limitado a aquellos con una necesidad relacionada con sus funciones. **Objetivo del Enfoque Personalizado** El personal no autorizado no tendrá acceso a los registros de actividades almacenados.	**Procedimientos de Prueba de Enfoques Definidos** **10.3.1** Entreviste a los administradores del sistema y examine las configuraciones y los privilegios del sistema para verificar que solo las personas con una necesidad relacionada con sus funciones tengan acceso de lectura a los archivos de registro de auditoría.	**Objetivo** Los archivos de registros de auditoría contienen información confidencial y el acceso de lectura a los archivos de registro debe limitarse solo a aquellos con una necesidad de negocio válida. Este acceso incluye archivos de registro de auditoría en los sistemas de origen, así como en cualquier otro lugar donde estén almacenados. **Buenas Prácticas** La protección adecuada de los registros de auditoría incluye un fuerte control de acceso que limite el acceso a los registros basándose únicamente en la "necesidad de saber" y el uso de segregación física o de red para hacer que los registros sean más difíciles de encontrar y modificar.
Requisitos del Enfoque Definido **10.3.2** Los archivos de registros de auditoría están protegidos para evitar modificaciones por parte de terceros. **Objetivo del Enfoque Personalizado** El personal no puede modificar los registros de actividad almacenados.	**Procedimientos de Prueba del Enfoque Definido** **10.3.2** Evalúe las configuraciones y privilegios del sistema y entreviste a los administradores para verificar que los archivos de registro de auditoría actuales estén protegidos contra modificaciones por parte de terceros a través de mecanismos de control de acceso, segregación física y/o segregación de red.	**Objetivo** A menudo, personas malintencionadas que han entrado en la red intentarán editar los registros de auditoría para ocultar su actividad. Sin la protección adecuada no se puede garantizar la totalidad, precisión e integridad de los registros de auditoría, y estos pueden volverse inútiles como herramienta de investigación después de un evento comprometedor. Por lo tanto, los registros de auditoría deben protegerse en los sistemas de origen, así como en cualquier otro lugar donde se almacenen. **Buenas Prácticas** Las entidades deben evitar que los registros se expongan en lugares accesibles al público.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **10.3.3** Los archivos de registros de auditoría, incluidos los de tecnologías externas, se respaldan de inmediato en un servidor de registro interno seguro, central o sobre otro medio que sea difícil de modificar. **Objetivo del Enfoque Personalizado** Los registros de actividad almacenados se protegen y conservan en una ubicación central para evitar modificaciones no autorizadas.	**Procedimientos de Prueba del Enfoque Definido** **10.3.3** Evalúe las configuraciones de apoyo o los archivos de registro para verificar que los archivos de registro de auditoría actuales, incluyendo los de tecnologías externas, se respalden de inmediato en un servidor de registros interno seguro u otro medio que sea difícil de modificar.	**Objetivo** Realizar una copia de seguridad de los registros rápidamente en un servidor de registros centralizado o en un medio que sea difícil de alterar mantiene los registros protegidos, incluso si el sistema que genera los registros se ve comprometido. La escritura de registros de tecnologías externas, como inalámbricas, controles de seguridad de red, DNS y servidores de correo, reduce el riesgo de que los registros se pierdan o sean alterados. **Buenas Prácticas** Cada entidad determina la mejor manera de realizar copias de seguridad de los archivos de registro, ya sea a través de uno o más servidores de registro centralizados u otros medios seguros. Los registros se pueden escribir directamente, descargar o copiar desde sistemas externos al sistema interno seguro o al medio.
Requisitos del Enfoque Definido **10.3.4** Los mecanismos de detección de cambios o supervisión de la integridad de los archivos se utilizan en registros de auditoría para garantizar que los datos de registros existentes no se puedan modificar sin generar alertas. **Objetivo del Enfoque Personalizado** Los registros de actividad almacenados no se pueden modificar sin que se genere una alerta.	**Procedimientos de Prueba del Enfoque Definido** **10.3.4** Evalúe la configuración del sistema, los archivos monitoreados y los resultados de las actividades de monitoreo, para verificar el uso del software de supervisión de integridad de los archivos o de detección de cambios en los registros de auditoría.	**Objetivo** Los sistemas de monitoreo de integridad de archivos o detección de cambios verifican cambios en archivos críticos y notifican cuando se identifican dichos cambios. La entidad generalmente monitorea los archivos que no cambian regularmente con propósitos de monitoreo de su integridad; pero cuando se reflejan cambios, indican un posible evento comprometedor. **Buenas Prácticas** El software utilizado para monitorear los cambios en los registros de auditoría debe configurarse para proporcionar alertas cuando se modifiquen o se eliminen los datos o archivos del registro existente. Sin embargo, los nuevos datos de registro que se agreguen a un registro de auditoría, no deberían generar una alerta.

Requisitos y Procedimientos de Prueba		Guía
10.4 Los registros de auditoría se revisan para identificar anomalías o actividades sospechosas.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
10.4.1 Los siguientes registros de auditoría se revisan 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, controles de seguridad de red, sistemas de detección de intrusiones/sistemas de prevención de intrusiones (IDS / IPS), servidores de autenticación).	**10.4.1.a** Evalúe las políticas y los procedimientos de seguridad para verificar que los procesos estén definidos para revisar todos los elementos especificados en este requisito al menos una vez al día. **10.4.1.b** Observe los procesos y entreviste al personal para verificar que todos los elementos especificados en este requisito se revisen al menos una vez al día.	**Objetivo** Muchas infracciones ocurren meses antes de ser detectadas. Las revisiones periódicas de los registros significan que los incidentes se pueden identificar rápidamente y abordar de manera proactiva. **Buenas Prácticas** La verificación de los registros a diario (los 7 días de la semana, los 365 días del año, incluidos los feriados) minimiza el tiempo y la exposición de una posible infracción. Las herramientas de recolección, análisis y alerta de registros, los sistemas de administración de registros centralizados, los analizadores de registros de eventos y las soluciones de administración de eventos e información de seguridad (SIEM) son ejemplos de herramientas automatizadas que se pueden utilizar para cumplir con este requisito. La revisión diaria de eventos de seguridad, por ejemplo, notificaciones o alertas que identifican actividades sospechosas o anormales, así como los registros de componentes críticos del sistema y registros de sistemas que realizan funciones de seguridad, como *firewall*, IDS/IPS, sistemas de monitoreo de integridad de archivos (FIM), etc., es necesaria para identificar problemas potenciales. La determinación de lo que es un "evento de seguridad" variará de una organización a otra y puede incluir la consideración del tipo de tecnología, ubicación y función del dispositivo. Las organizaciones también pueden mantener un punto de referencia de lo que es tráfico "normal" para ayudar a identificar comportamientos anormales. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Las actividades potencialmente sospechosas o anómalas se identifican rápidamente para minimizar su impacto.		Una entidad que utiliza proveedores de servicios de terceros para realizar servicios de revisión de registros tiene la responsabilidad de proporcionar un contexto del entorno de la entidad a los proveedores de servicios, de manera que estos comprendan ese entorno, tenga un punto de referencia de lo que es el tráfico "normal" para la entidad, y puedan detectar posibles problemas de seguridad y proporcionar excepciones precisas y notificar anomalías.
Requisitos del Enfoque Definido **10.4.1.1** Se utilizan mecanismos automatizados para realizar revisiones de los registros de auditoría. **Objetivo del Enfoque Personalizado** Las actividades potencialmente sospechosas o anormales se identifican mediante un mecanismo repetible y coherente. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba del Enfoque Definido** **10.4.1.1** Evalúe los mecanismos de revisión y entreviste al personal para verificar que se utilicen mecanismos automatizados para realizar las revisiones de los registros.	**Objetivo** Las revisiones de registros manuales son difíciles de realizar, incluso para uno o dos sistemas, debido a la cantidad de datos de registros que se generan. Sin embargo, el uso de herramientas de recolección, análisis y alerta de registros, sistemas de administración de registros centralizados, analizadores de registros de eventos y soluciones de administración de eventos e información de seguridad (SIEM) puede ayudar a facilitar el proceso al identificar los eventos de registro que deban revisarse. **Buenas Prácticas** La entidad debe mantener las herramientas de registro alineadas con cualquier cambio en su entorno mediante la revisión periódica de la configuración de herramientas y la actualización de la configuración para reflejar cualquier cambio.
Requisitos del Enfoque Definido **10.4.2** Los registros de todos los demás componentes del sistema (aquellos no especificados en el Requisito 10.4.1) se revisan periódicamente.	**Procedimientos de Prueba del Enfoque Definido** **10.4.2.a** Evalúe las políticas y los procedimientos de seguridad para verificar que los procesos estén definidos para la revisión de los registros de todos los demás componentes del sistema periódicamente.	**Objetivo** La revisión periódica de los registros de todos los demás componentes del sistema (no especificados en el Requisito 10.4.1) ayuda a identificar indicaciones de posibles problemas o intentos de acceso a sistemas críticos a través de sistemas menos críticos.

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Las actividades potencialmente sospechosas o anormales para otros componentes del sistema (no incluidas en 10.4.1) se revisan de acuerdo con el riesgo identificado por la entidad. **Notas de Aplicabilidad** Este requisito es aplicable a todos los demás componentes del sistema dentro del alcance no incluidos en el Requisito 10.4.1.	**10.4.2.b** Evalúe los resultados documentados de las revisiones de los registros y entreviste al personal para verificar que las revisiones de los registros se realicen periódicamente.	
Requisitos del Enfoque Definido **10.4.2.1** La frecuencia de las evaluaciones periódicas de los componentes del sistema identificados (No definidos en el Requisito 10.4.1) se define en el análisis de riesgo específico de la entidad, el cual se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1 **Objetivo del Enfoque Personalizado** Las revisiones de registros para los componentes del sistema de menor riesgo se realizan con una frecuencia que aborda el riesgo de la entidad. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba del Enfoque Definido** **10.4.2.1.a** Evalúe el análisis de riesgo específico de la entidad para conocer la frecuencia de las evaluaciones periódicas para todos los otros componentes del sistema (no definidos en el Requisito 10.4.1) a fin de verificar que el análisis de riesgo se realizó de acuerdo con todos los elementos especificados en el Requisito 12.3.1. **10.4.2.1.b** Evalúe los resultados documentados de las evaluaciones periódicas de todos los otros componentes del sistema (no definidos en el Requisito 10.4.1) y entreviste al personal para verificar que las evaluaciones se realicen con la frecuencia especificada en el análisis de riesgo específico de la entidad para este requisito.	**Objetivo** Las entidades pueden determinar el período óptimo de revisión de estos registros basándose en criterios como la complejidad del entorno de cada entidad, el número de tipos de sistemas que deben examinarse y las funciones de dichos sistemas.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Si no se investigan las excepciones y anomalías identificadas durante el proceso de revisión de registros, es posible que la entidad no tenga conocimiento de actividades no autorizadas y potencialmente peligrosas que ocurren dentro de su red. **Buenas Prácticas** Las entidades deben considerar cómo abordar lo siguiente al desarrollar sus procesos para definir y administrar excepciones y anomalías: • ¿Cómo se registran las actividades de análisis de registros?, • ¿Cómo clasificar y priorizar las excepciones y anomalías?, • ¿Qué procedimientos deben establecerse para informar y escalar las excepciones y anomalías?, y • Quién es responsable de la investigación y de las tareas de corrección.
10.4.3 Se abordan las excepciones y anomalías identificadas durante el proceso de revisión.	**10.4.3.a** Evalúe las políticas y los procedimientos de seguridad para verificar que se definen los procesos que abordan las excepciones y las anomalías identificadas durante el proceso de revisión.	
	10.4.3.b Observe los procesos y entreviste al personal para verificar que, cuando se identifican excepciones y anomalías, éstas son abordadas.	
Objetivo del Enfoque Personalizado		
Se abordan las actividades sospechosas o anormales.		

Requisitos y Procedimientos de Prueba		Guía
10.5 Se conserva el historial del registro de auditoría y está disponible para su análisis.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Buenas Prácticas**
10.5.1 Conserve el historial de los registros de auditoría durante 12 meses como mínimo, teniendo al menos los tres últimos meses inmediatamente disponibles para su análisis.	**10.5.1.a** Evalúe la documentación para verificar que se ha definido lo siguiente: • Políticas de retención de registros de auditoría. • Procedimientos para conservar el historial de los registros de auditoría durante al menos 12 meses, teniendo al menos los tres últimos meses inmediatamente disponibles en línea.	Es necesario conservar el historial de los registros de auditoría durante al menos 12 meses, ya que las infracciones suelen pasar desapercibidas durante mucho tiempo. Disponer de un historial de registros almacenado de forma centralizada facilita a los investigadores determinar el momento en el que se produjeron las infracciones potenciales y cuáles son los posibles sistemas afectados. Al tener tres meses de registros disponibles inmediatamente, la entidad puede identificar rápidamente y minimizar el impacto de una violación de los datos. **Ejemplos** Los métodos que permiten que los registros estén disponibles inmediatamente incluyen el almacenamiento de registros en línea, el archivo de registros o la restauración rápida de registros a partir de copias de apoyo.
	10.5.1.b Evalúe las configuraciones del historial de registros de auditoría, entreviste al personal y analizar los registros de auditoría para verificar que el historial de registros de auditoría se conserva durante al menos 12 meses.	
Objetivo del Enfoque Personalizado	**10.5.1.c** Entreviste al personal y observe los procesos para verificar que el historial de registros de auditoría de los tres últimos meses como mínimo, esté disponible de inmediato para su análisis.	
Los registros históricos de actividad están disponibles inmediatamente para respaldar la respuesta a incidentes y se conservan al menos durante 12 meses.		

Requisitos y Procedimientos de Prueba		Guía
10.6 Los mecanismos de sincronización de la hora admiten una configuración de hora coherente en todos los sistemas.		
Requisitos del Enfoque Definido **10.6.1** Los relojes del sistema y la hora están sincronizados usando tecnología de sincronización de tiempo. **Objetivo del Enfoque Personalizado** La hora en común se establece en todos los sistemas. **Notas de Aplicabilidad** Mantener actualizada la tecnología de sincronización horaria incluye la aplicación de parches como lo establecen los Requisitos 6.3.1 y 6.3.3 PCI DSS.	**Procedimientos de Prueba del Enfoque Definido** **10.6.1** Evalúe los ajustes de configuración para verificar que la tecnología de sincronización de tiempo está implementada y se mantiene actualizada.	**Objetivo** La tecnología de sincronización horaria se utiliza para sincronizar los relojes de varios sistemas. Cuando los relojes no están correctamente sincronizados, puede ser difícil, si no imposible, comparar los archivos de registro de diferentes sistemas y establecer una secuencia exacta de eventos, lo que es crucial para el análisis forense después de una brecha. Para los equipos forenses post-incidentes, la precisión y la coherencia de la hora en todos los sistemas y la hora de cada actividad son esenciales para determinar cómo se vieron comprometidos los sistemas. **Ejemplos** El Protocolo de Tiempo de Red (NTP) es un ejemplo de tecnología de sincronización de tiempo.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
10.6.2 Los sistemas están configurados con la hora correcta y consistente como sigue: • Uno o más servidores de tiempo designados están en uso. • Solo los servidores de hora central designados reciben la hora de fuentes externas. • La hora recibida de fuentes externas se basa en la Hora Atómica Internacional u Hora Universal Coordinada (UTC). • Los servidores de tiempo designados aceptan actualizaciones de tiempo solo de fuentes externas específicas aceptadas por la industria. • Cuando hay más de un servidor de tiempo designado, los servidores de tiempo se emparejan entre sí para mantener la hora exacta. • Los sistemas internos reciben información de la hora solo de los servidores de hora central designados.	**10.6.2** Evalúe los ajustes de configuración del sistema para adquirir, distribuir y almacenar la hora correcta a fin de verificar que los ajustes estén configurados de acuerdo con todos los elementos especificados en este requisito.	El uso de servidores de tiempo de buena reputación es un componente crítico del proceso de sincronización de tiempo. Aceptar las actualizaciones horarias de fuentes externas específicas y aceptadas por la industria, ayuda a evitar que individuos malintencionados cambien la configuración horaria de los sistemas. **Buenas Prácticas** Otra opción para evitar el uso no autorizado de los servidores de hora internos es cifrar las actualizaciones con una clave simétrica y crear listas de control de acceso que especifiquen las direcciones IP de los equipos del cliente a los cuales se les proporcionarán las actualizaciones horarias.
Objetivo del Enfoque Personalizado		
La hora en todos los sistemas es precisa y coherente.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
10.6.3 La configuración de sincronización de la hora y los datos están protegidos de la siguiente manera: • El acceso a los datos de tiempo está restringido solo al personal con una necesidad de negocio. • Cualquier cambio en la configuración de tiempo en sistemas críticos se registra, monitorea y verifica.	**10.6.3.a** Evalúe las configuraciones del sistema y los ajustes de sincronización de tiempo para verificar que el acceso a los datos de tiempo esté restringido solo al personal con una necesidad de negocio.	Los atacantes intentarán cambiar las configuraciones de tiempo para ocultar sus actividades. Por lo tanto, restringir la capacidad de cambiar o modificar las configuraciones de sincronización de hora o la hora del sistema a los administradores reducirá la probabilidad de que un atacante cambie con éxito las configuraciones de hora.
	10.6.3.b Evalúe las configuraciones del sistema y los ajustes y registros de sincronización de la hora y observe los procesos para verificar que cualquier cambio en la configuración de la hora en los sistemas críticos se registre, supervise y revise.	
Objetivo del Enfoque Personalizado		
La configuración de la hora del sistema no puede ser modificada por personal no autorizado.		

Requisitos y Procedimientos de Prueba		Guía
10.7 Las fallas de los sistemas de control de seguridad críticos se detectan, informan y atienden con prontitud.		
Requisitos del Enfoque Definido **10.7.1** ***Requisito Adicional solo para proveedores de servicios:*** Las fallas de los sistemas de control de seguridad críticos se detectan, alertan y abordan de inmediato, incluyendo entre otras, las fallas de los siguientes sistemas de control de seguridad críticos: • Controles de seguridad de la red • IDS/IPS • FIM • Soluciones antimalware: • Controles de acceso físico • Controles de Ingreso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan) **Objetivo del Enfoque Personalizado** Las fallas en los sistemas críticos de control de seguridad se identifican y abordan de inmediato. **Notas de Aplicabilidad** Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios.	**Procedimientos de Prueba del Enfoque Definido** **10.7.1.a** ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Evalúe la documentación para verificar que los procesos estén definidos para la rápida detección y el tratamiento de fallas de los sistemas críticos de control de seguridad, incluyendo, entre otros, fallas de todos los elementos especificados en este requisito. **10.7.1.b** ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Observe los procesos de detección y alerta y entreviste al personal para verificar que las fallas de los sistemas de control de seguridad críticos son detectados y notificados, y que la falla de un control de seguridad crítico genere una alerta.	**Objetivo** Sin procesos formales para detectar y lanzar alertas cuando fallan los controles de seguridad críticos, las fallas pueden pasar desapercibidas durante períodos prolongados y brindar a los atacantes tiempo suficiente para comprometer los componentes del sistema y robar datos de cuentas del CDE. **Buenas Prácticas** Los tipos específicos de fallas pueden variar dependiendo de la función del componente del sistema del dispositivo y la tecnología en uso. Las fallas típicas incluyen que el sistema cese de realizar sus funciones de seguridad o que no funcione de la manera prevista, como un cortafuego que borra todas sus reglas o se desconecta.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
10.7.2 Las fallas de los sistemas de control de seguridad críticos se detectan, alertan y abordan de inmediato, incluidas, entre otras, las fallas de los siguientes sistemas de control de seguridad críticos: • Controles de seguridad de la red • IDS/IPS • Cambiar los mecanismos de detección • Soluciones antimalware: • Controles de acceso físico • Controles de Ingreso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan) • Mecanismos de revisión del registro de auditoría. • Herramientas de prueba de seguridad automatizadas (si se utilizan)	**10.7.2.a** Evalúe la documentación para verificar que los procesos estén definidos para la detección rápida y el tratamiento de fallas de los sistemas de control de seguridad críticos, incluyendo, pero no limitado a fallas de todos los elementos especificados en este requisito.	Sin procesos formales para detectar y lanzar alertas cuando fallan los controles de seguridad críticos, las fallas pueden pasar desapercibidas durante períodos prolongados y brindar a los atacantes tiempo suficiente para comprometer los componentes del sistema y robar datos de cuentas del CDE. **Buenas Prácticas** Los tipos específicos de fallas pueden variar dependiendo de la función del componente del sistema del dispositivo y la tecnología en uso. Sin embargo, las fallas típicas incluyen un sistema que ya no realiza su función de seguridad o que no funciona de la manera prevista, por ejemplo, un cortafuego que borra sus reglas o se desconecta.
Objetivo del Enfoque Personalizado	**10.7.2.b** Observe los procesos de detección y alerta y entreviste al personal para verificar que las fallas de los sistemas de control de seguridad críticos se detecten y notifiquen, y que la falla de un control de seguridad crítico dé como resultado la generación de una alerta.	
Las fallas en los sistemas críticos de control de seguridad se identifican y abordan de inmediato.		
Notas de Aplicabilidad		
Este requisito se aplica únicamente cuando la entidad evaluada es un proveedor de servicios. Este requisito será sustituido por el requisito 10.7.2 a partir del 31 de marzo de 2025.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
10.7.3 Las fallas de cualquier sistema de control de seguridad crítico se responden con prontitud, incluidas, entre otras, las siguientes: • Restaurando las funciones de seguridad. • Identificando y documentando la duración (fecha y hora de principio a fin) de la falla de seguridad. • Identificando y documentando las causas de las fallas y documentando el remedio requerido. • Identificando y abordando cualquier problema de seguridad que surgió durante la falla. • Determinar si se requieren más acciones como resultado de la falla de seguridad. • Implementar controles para evitar que se repita la causa de la falla. • Reanudación del monitoreo de los controles de seguridad.	**10.7.3.a** Evalúe la documentación y entreviste al personal para verificar que los procesos estén definidos e implementados para responder a fallas dentro de cualquier sistema de control de seguridad crítico e incluir al menos todos los elementos especificados en este requisito.	Si las alertas de fallas de los sistemas de control de seguridad críticos no se responden de manera rápida y efectiva, los atacantes pueden usar este tiempo para insertar software malicioso, obtener el control de un sistema, o robar datos del entorno de la entidad. **Buenas Prácticas** La evidencia documentada (por ejemplo, los registros dentro de un sistema de gestión de problemas) debe proporcionar el apoyo de que existen procesos y procedimientos para responder a las fallas de seguridad. Además, el personal debe conocer sus responsabilidades en caso de fallas. Las acciones y respuestas a las fallas deben capturarse en la evidencia documentada.
Objetivo del Enfoque Personalizado	**10.7.3.b** Evalúe los registros para verificar que las fallas en los sistemas críticos de control de seguridad estén documentadas para incluir: • Identificación de las causas del fallo. • Duración (fecha y hora de inicio y finalización) del fallo de seguridad. • Detalles de la rehabilitación necesaria para abordar raíz del problema.	
Las fallas en los sistemas de control de seguridad críticos se analizan, se controlan y resuelven; y los controles de seguridad se restauran para minimizar el impacto. Se abordan los problemas de seguridad resultantes y se toman medidas para evitar que vuelvan a ocurrir.		

(continúa en la página siguiente)

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito se aplica únicamente cuando la entidad evaluada es un proveedor de servicios hasta el 31 de marzo de 2025, fecha a partir de la cual este requisito se aplicará a todas las entidades. *Este es un requisito actual de la versión 3.2.1 que aplica solo a los proveedores de servicios. Sin embargo, este requisito es una práctica recomendada para todas las demás entidades hasta el 31 de marzo de 2025, después de lo cual será obligatoria y debe considerarse en su totalidad durante una evaluación PCI DSS*.		

Requisito 11: Poner a Prueba Regularmente la Seguridad de los Sistemas y de las Redes

Secciones	
11.1	Se definen y comprenden los procesos y mecanismos para probar periódicamente la seguridad de los sistemas y redes.
11.2	Los puntos de acceso inalámbrico se identifican y monitorean, y se abordan los puntos de acceso inalámbrico no autorizados.
11.3	Las vulnerabilidades internas y externas se identifican regularmente, son priorizadas y atendidas.
11.4	Las pruebas de penetración externas e internas se realizan regularmente y las vulnerabilidades explotables y las debilidades en materia de seguridad son corregidas.
11.5	Las intrusiones en la red y los cambios de archivos inesperados se detectan y responden.
11.6	Los cambios no autorizados en las páginas de pago se detectan y responden.

Descripción
Las vulnerabilidades son descubiertas continuamente por investigadores y por personas malintencionadas, y son introducidas en un nuevo software. Los componentes del sistema, los procesos y el software personalizado y a medida deben probarse con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno cambiante. Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
11.1 Se definen y comprenden los procesos y mecanismos para probar periódicamente la seguridad de los sistemas y redes.		
Requisitos del Enfoque Definido **11.1.1** Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 11 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas. **Objetivo del Enfoque Personalizado** Las expectativas, los controles y la vigilancia en el cumplimiento con las actividades dentro del Requisito 11 están definidos y son cumplidos por el personal afectado. Todas las actividades de apoyo son repetibles, se aplican de manera consistente y se ajustan a la intención de la gerencia.	**Procedimientos de Prueba del Enfoque Definido** **11.1.1** Evalúe la documentación y entreviste al personal para verificar que las políticas de seguridad y los procedimientos operativos son administrados de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** El Requisito 11.1.1 trata sobre la gestión y el mantenimiento eficiente de las diversas políticas y procedimientos especificados en el Requisito 11. Si bien es importante definir las políticas o procedimientos específicos mencionados en el Requisito 11, es igualmente importante garantizar que se documenten, se mantengan y se difundan adecuadamente. **Buenas Prácticas** Es importante actualizar las políticas y los procedimientos según sea necesario para abordar los cambios en los procesos, las tecnologías y los objetivos de negocios. Por esta razón, considere actualizar estos documentos lo más pronto posible después de que haya ocurrido un cambio y no solo en ciclos periódicos. **Definiciones** Las Políticas de Seguridad definen los objetivos y principios de seguridad de la entidad. Los procedimientos operativos describen cómo desarrollar las actividades y definen los controles, métodos y procesos que se siguen para lograr el resultado deseado de forma coherente y de acuerdo con los objetivos de la política.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Si los roles y responsabilidades no se asignan formalmente, es posible que el personal no esté al tanto de sus responsabilidades diarias y que las actividades críticas no ocurran. **Buenas Prácticas** Los roles y responsabilidades pueden documentarse dentro de políticas y procedimientos o mantenerse en documentos separados. Como parte de los roles de comunicación y de las responsabilidades, las entidades pueden considerar pedir al personal que confirme su aceptación y comprensión de sus roles y las responsabilidades asignadas. **Ejemplos** Un método para documentar roles y responsabilidades es una matriz de asignación de responsabilidades que indica quién está a cargo, quién es el responsable, la persona consultada y la persona informada (también llamada matriz RACI).
11.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 11 son documentadas, asignadas y entendidas.	**11.1.2.a** Evalúe la documentación para verificar que las descripciones de los roles y responsabilidades para realizar las actividades del Requisito 11 estén documentadas y asignadas.	
	11.1.2.b Entreviste al personal responsable de desarrollar las actividades del Requisito 11 para verificar que los roles y responsabilidades se asignen según sean documentadas y entendidas.	
Objetivo del Enfoque Personalizado		
Se asignan las responsabilidades diarias para realizar todas las actividades del Requisito 11. El personal es responsable del funcionamiento exitoso y continuo de estos requisitos.		

Requisitos y Procedimientos de Prueba		Guía
11.2 Se identifican y controlan los puntos de acceso inalámbricos y se abordan los puntos de acceso inalámbricos no autorizados.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.2.1 Los puntos de acceso inalámbricos autorizados y no autorizados se gestionan de la siguiente manera: • Se comprueba la existencia de puntos de acceso inalámbricos *(Wi-Fi)* para, • Detectar e identificar todos los puntos de acceso inalámbricos autorizados y no autorizados, • Que la verificación, detección e identificación ocurre al menos cada tres meses. • Si se utiliza la supervisión automatizada, se notifica al personal mediante la generación de alertas.	**11.2.1.a** Evalúe las políticas y los procedimientos para verificar que los procesos están definidos para gestionar los puntos de acceso inalámbricos tanto autorizados y no autorizados con todos los elementos especificados en este requisito. **11.2.1.b** Evalúe las metodologías en uso y la documentación resultante, y entreviste al personal para verificar que se han definido los procesos para detectar e identificar tanto los puntos de acceso inalámbricos autorizados como los no autorizados, de acuerdo con todos los elementos especificados en este requisito. **11.2.1.c** Evalúe los resultados de la evaluación inalámbrica y entreviste al personal para verificar que las evaluaciones inalámbricas se realizaron de acuerdo con todos los elementos especificados en este requisito. **11.2.1.d** Si se utiliza el monitoreo automatizado, examine los ajustes de configuración para verificar que la configuración generará alertas para notificar al personal.	La implementación y /o explotación de la tecnología inalámbrica dentro de una red es una vía común para que individuos malintencionados ingresen a la red y a los datos de titulares de tarjetas. Los dispositivos inalámbricos no autorizados podrían estar ocultos dentro de un ordenador u otro componente del sistema, o conectados a él. Estos dispositivos también podrían estar conectados directamente a un puerto de red, a un dispositivo de red como un conmutador o un enrutador, o insertados en forma de tarjeta de interfaz inalámbrica dentro de un componente del sistema. Si un dispositivo o red inalámbrica se instala sin el conocimiento de la empresa, esto puede permitir a un atacante entrar en la red de forma fácil e "invisible". Detectar y eliminar estos puntos de acceso no autorizados reduce la duración y la probabilidad de que estos dispositivos sean aprovechados para un ataque. **Buenas Prácticas** El tamaño y la complejidad de un entorno dictarán las herramientas y los procesos apropiados que se utilizarán para proporcionar suficiente garantía de que no se ha instalado un punto de acceso inalámbrico fraudulento en el entorno. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado		
Los puntos de acceso inalámbricos no autorizados se identifican y abordan periódicamente.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito aplica incluso cuando existe una política que prohíbe el uso de la tecnología inalámbrica, ya que los atacantes no leen ni siguen la política de la empresa. Los métodos utilizados para cumplir este requisito deben ser suficientes para detectar e identificar tanto los dispositivos autorizados como los no autorizados, incluidos los dispositivos no autorizados conectados a dispositivos que sí están autorizados.		Por ejemplo, realizar una inspección física detallada de un quiosco de venta al por menor en un centro comercial, donde todos los componentes de comunicación están dentro de carcasas resistentes a la manipulación y a prueba de manipulaciones, puede ser suficiente para garantizar que no se ha conectado o instalado un punto de acceso inalámbrico fraudulento. Sin embargo, en un entorno con varios nodos (como en una gran tienda minorista, un centro de llamadas, una sala de servidores o un centro de datos), la inspección física detallada puede ser difícil. En ese caso se pueden combinar varios métodos, como hacer inspecciones físicas del sistema junto con los resultados de un analizador inalámbrico. **Definiciones** También se denomina detección de puntos de acceso fraudulentos. **Ejemplos** Los métodos que pueden utilizarse incluyen, entre otros, los escaneos de redes inalámbricas, las inspecciones físicas/lógicas de los componentes del sistema y su infraestructura, el control de acceso a la red (NAC) o los IDS/IPS inalámbricos. El NAC y los IDS/IPS inalámbricos son ejemplos de herramientas de supervisión automatizada

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Un inventario de puntos de acceso inalámbricos autorizados puede ayudar a los administradores a responder rápidamente cuando se detectan puntos de acceso inalámbricos no autorizados. Esto ayuda a minimizar de forma proactiva la exposición del CDE a individuos malintencionados. **Buenas Prácticas** Si utiliza un escáner inalámbrico, es igualmente importante tener una lista definida de puntos de acceso conocidos que, aunque no estén conectados a la red de la empresa, generalmente se detectarán durante un escaneo. Estos dispositivos que no propiedad de la empresa, se encuentran frecuentemente en edificios con varios inquilinos o negocios ubicados uno cerca del otro. Sin embargo, es importante verificar que estos dispositivos no estén conectados al puerto de red de la entidad o a través de otro dispositivo conectado a la red y que tengan un SSID parecido al de otro negocio cercano. Los resultados del escaneo deben tener en cuenta dichos dispositivos y cómo se determinó que estos dispositivos podrían ser "ignorados". Además, la detección de cualquier punto de acceso inalámbrico no autorizado que sea identificado como amenaza para el CDE debe gestionarse siguiendo el plan de respuesta a incidentes de la entidad según el Requisito 12.10.1.
11.2.2 Se mantiene un inventario de los puntos de acceso inalámbricos autorizados, incluyendo una justificación de negocio documentada.	**11.2.2** Evalúe la documentación para verificar que se mantenga un inventario de puntos de acceso inalámbricos autorizados y que se documente una justificación de negocio para todos los puntos de acceso inalámbricos autorizados.	
Objetivo del Enfoque Personalizado		
Los puntos de acceso inalámbrico no autorizados no se confunden con los puntos de acceso inalámbrico autorizados.		

Requisitos y Procedimientos de Prueba		Guía
11.3 Las vulnerabilidades externas e internas se identifican, se priorizan y se abordan periódicamente.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
11.3.1 Los escaneos de vulnerabilidades internas se realizan de la siguiente manera: • Al menos una vez cada tres meses. • Se resuelven las vulnerabilidades críticas y de alto riesgo (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1). • Se realizan re-escaneos que confirman que se han resuelto todas las vulnerabilidades críticas y de alto riesgo (como se indicó anteriormente). • La herramienta de escaneo se mantiene actualizada con la información más reciente sobre vulnerabilidades. • Los escaneos son realizados por personal calificado con la independencia organizacional del probador.	**11.3.1.a** Evalúe los resultados del informe de escaneo interno de los últimos 12 meses para verificar que los escaneos internos se hayan realizado al menos una vez cada tres meses en el período de los 12 meses más recientes. **11.3.1.b** Evalúe los resultados del informe de escaneo interno de cada escaneo y vuelva a realizar el escaneo en los últimos 12 meses para verificar que se hayan resuelto todas las vulnerabilidades críticas y de alto riesgo (identificadas en el Requisito 6.3.1 PCI DSS). **11.3.1.c** Evalúe las configuraciones de la herramienta de escaneo y entreviste al personal para verificar que la herramienta de escaneo se mantenga actualizada con la información de vulnerabilidad más reciente. **11.3.1.d** Entreviste al personal responsable para verificar que el escaneo fue realizado por un recurso interno calificado o un tercero externo calificado y que existe independencia organizacional del asesor.	**Objetivo** Identificar y abordar las vulnerabilidades rápidamente reduce la probabilidad de que se explote una vulnerabilidad al igual que el riesgo potencial de un componente del sistema o de los datos del titular de la tarjeta. Los escaneos de vulnerabilidades realizados al menos cada tres meses proporcionan esta detección e identificación. **Buenas Prácticas** Las vulnerabilidades que presentan el mayor riesgo para el entorno (por ejemplo, clasificadas como altas o críticas según el Requisito 6.3.1) deben resolverse con máxima prioridad. Se pueden combinar varios informes de escaneo para el proceso de escaneo trimestral, a fin de demostrar que todos los sistemas fueron escaneos y todas las vulnerabilidades aplicables fueron resueltas como parte del ciclo de escaneo de vulnerabilidades de tres meses. Sin embargo, es posible que se requiera documentación adicional para verificar que las vulnerabilidades no reparadas estén en proceso de resolución. Si bien se requieren escaneos al menos una vez cada tres meses, se recomienda realizar escaneos más frecuentes según la complejidad de la red, la frecuencia de los cambios y los tipos de dispositivos, software y sistemas operativos utilizados. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado La postura de seguridad de todos los componentes del sistema se verifica periódicamente utilizando herramientas automatizadas diseñadas para detectar vulnerabilidades que operan dentro de la red. Las vulnerabilidades detectadas se evalúan y rectifican sobre la base de un marco formal de evaluación de riesgos. **Notas de Aplicabilidad** No es necesario utilizar un QSA o un ASV para realizar escaneos internos de vulnerabilidades. Los escaneos de vulnerabilidades internas pueden ser realizados por personal interno calificado que sea razonablemente independiente de los componentes del sistema que se analizan (por ejemplo, un administrador de red no debería ser responsable de analizar la red), o una entidad puede optar por una empresa especializada en escaneos de vulnerabilidades		**Definiciones** Un escaneo de vulnerabilidades es una combinación de herramientas, técnicas y/o métodos automatizados que se ejecutan en dispositivos y servidores internos y externos diseñados para exponer potenciales vulnerabilidades en aplicaciones, sistemas operativos y dispositivos de red, que podrían ser encontrados por personas malintencionadas.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.3.1.1 Todas las demás vulnerabilidades aplicables (aquellas que no se clasifican como de alto riesgo o críticas (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1) se gestionan de la siguiente manera: • Abordado en función del riesgo definido en el análisis de riesgo específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1. • Los re-escaneos se realizan según sea necesario.	**11.3.1.1.a** Evalúe el análisis de riesgo específico de la entidad que define el riesgo de abordar todas las demás vulnerabilidades aplicables (aquellas que no están clasificadas como de alto riesgo o críticas según la clasificación de riesgo de vulnerabilidad de la entidad en el Requisito 6.3.1) para verificar que el análisis de riesgo se realizó de acuerdo con todos los elementos especificados en el Requisito 12.3.1.	Todas las vulnerabilidades, independientemente de su criticidad, proporcionan una vía potencial de ataque y, por lo tanto, deben abordarse periódicamente, y las vulnerabilidades que exponen el mayor riesgo se abordan más rápidamente para limitar la posible ventana de ataque.
Objetivo del Enfoque Personalizado Las vulnerabilidades de menor clasificación (más bajas que altas o críticas) se abordan con una frecuencia de acuerdo con el riesgo de la entidad.	**11.3.1.1.b** Entreviste al personal responsable y examine los resultados del informe de escaneo interno u otra documentación para verificar que todas las demás vulnerabilidades aplicables (aquellas que no están clasificadas como de alto riesgo o críticas según la clasificación de riesgo de vulnerabilidad de la entidad en el Requisito 6.3. 1) se abordan en función del riesgo definido en el análisis de riesgo específico de la entidad, y que el proceso de escaneo incluye nuevas exploraciones según sea necesario para confirmar que se han abordado las vulnerabilidades.	
Notas de Aplicabilidad El plazo para abordar las vulnerabilidades de menor riesgo está sujeto a los resultados de un análisis de riesgo según el Requisito 12.3.1 que incluye (mínimamente) la identificación de los activos que se protegen, las amenazas y la probabilidad y / o el impacto de una amenaza que se realiza. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.3.1.2 Los escaneos de vulnerabilidades internas se realizan mediante escaneos autenticados como sigue: • Se documentan los sistemas que no pueden aceptar credenciales para el escaneo autenticado. • Se utilizan suficientes privilegios para aquellos sistemas que aceptan credenciales para escanear. • Si las cuentas utilizadas para el escaneo autenticado se pueden utilizar para el inicio de sesión interactivo, estas se gestionan de acuerdo con el Requisito 8.2.2.	**11.3.1.2.a** Evalúe las configuraciones de la herramienta de escaneo para verificar que el escaneo autenticado se utilice para escaneos internos, con suficientes privilegios para aquellos sistemas que aceptan credenciales para escaneo.	El escaneo autenticado proporciona una mayor comprensión del panorama de vulnerabilidades de una entidad, ya que puede detectar vulnerabilidades que los escaneos no autenticados no pueden detectar. Los atacantes pueden aprovechar las vulnerabilidades que una entidad desconoce porque ciertas vulnerabilidades solo se detectarán con un escaneo autenticado. El escaneo autenticado puede generar información adicional significativa sobre las vulnerabilidades de la organización.
	11.3.1.2.b Evalúe los resultados del informe de escaneo y entreviste al personal para verificar que se realicen escaneos autenticados.	**Buenas Prácticas**
Objetivo del Enfoque Personalizado	**11.3.1.2.c** Si las cuentas utilizadas para el escaneo autenticado se pueden usar para el inicio de sesión interactivo, examine las cuentas y entreviste al personal para verificar que las cuentas se administran siguiendo todos los elementos especificados en el Requisito 8.2.2.	Las credenciales utilizadas para estos escaneos deben considerarse como de privilegios elevados. Deben estar protegidos y controlados como tales, siguiendo los requisitos 7 y 8 PCI DSS (excepto los requisitos de autenticación de múltiples factores y las cuentas de aplicaciones y sistemas).
Las herramientas automatizadas que se utilizan para detectar vulnerabilidades pueden detectar vulnerabilidades locales en cada sistema que no son visibles de forma remota.	**11.3.1.2.d** Evalúe la documentación para verificar que se definen los sistemas que no pueden aceptar credenciales para el escaneo autenticado.	

(continúa en la página siguiente)

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad		
Las herramientas de escaneo autenticadas pueden estar basadas en host o en red. Los privilegios "suficientes" son los necesarios para ingresar a los recursos del sistema, de modo que se pueda realizar un análisis exhaustivo que detecte vulnerabilidades conocidas. Este requisito no se aplica a los componentes del sistema que no pueden aceptar credenciales para escanear. Algunos ejemplos de sistemas que pueden no aceptar credenciales para escanear incluyen algunos dispositivos de red y seguridad, servidores y contenedores. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.3.1.3 Los escaneos internos se realizan después de cualquier cambio significativo como sigue: • Se resuelven las vulnerabilidades críticas y de alto riesgo (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1). • Los re-escaneos se realizan según sea necesario. • Los escaneos son realizados por personal cualificado con la independencia organizacional del probador (no se requiere que sea un QSA o ASV).	**11.3.1.3.a** Evalúe la documentación de control de cambios y los informes de escaneo internos para verificar que los componentes del sistema fueron escaneos después de cualquier cambio significativo.	El escaneo de un entorno después de cualquier cambio significativo garantiza que los cambios se realizaron adecuadamente, de manera que la seguridad del entorno no se vio comprometida a causa del cambio. **Buenas Prácticas** Las entidades deberían realizar escaneos después de realizar cambios significativos como parte del proceso de cambio según el Requisito 6.5.2 y antes de considerar el cambio como completo. Todos los componentes del sistema afectados por el cambio deberán ser escaneos.
Objetivo del Enfoque Personalizado La postura de seguridad de todos los componentes del sistema se verifica tras la realización de cambios significativos en la red o en los sistemas, mediante el uso de herramientas automatizadas diseñadas para detectar las vulnerabilidades que operan dentro de la red. Las vulnerabilidades detectadas se evalúan y rectifican sobre la base de un marco formal de evaluación de riesgos.	**11.3.1.3.b** Entreviste al personal y examine los informes de escaneo y re-escaneo internos para verificar que se realizaron escaneos internos después de cambios significativos y que se resolvieron las vulnerabilidades críticas y de alto riesgo definidas en el Requisito 6.3.1.	
Notas de Aplicabilidad No se requiere el escaneo de vulnerabilidades internas autenticado según el Requisito 11.3.1.2 para los análisis realizados después de cambios significativos.	**11.3.1.3.c** Entreviste al personal para verificar que los escaneos internos son realizados por recursos internos calificados o por un tercero externo calificado y con la independencia organizacional del asesor.	

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **11.3.2** Los escaneos de vulnerabilidad externos se realizan de la siguiente manera: • Al menos una vez cada tres meses. • Por parte de un proveedor de Escaneo Aprobado por PCI SSC (ASV). • Las vulnerabilidades se resuelven y se cumple con los requisitos de la Guía del Programa ASV. • Se realizan nuevos escaneos según sea necesario para confirmar que las vulnerabilidades se han resuelto de acuerdo con los requisitos de la Guía del Programa ASV escaneos aprobados. **Objetivo del Enfoque Personalizado** Este requisito no es apto para el enfoque personalizado. **Notas de Aplicabilidad** Para el cumplimiento inicial PCI DSS no es necesario que se completen cuatro escaneos aprobados en un plazo de 12 meses si el asesor verifica que: 1) el resultado del escaneo más reciente fue un escaneo satisfactorio, 2) la entidad ha documentado políticas y procedimientos que requieren escaneos al menos una vez cada tres meses, y 3) las vulnerabilidades observadas en los resultados del escaneo se han corregido como se muestra en un re-escaneo. *(continúa en la página siguiente)*	**Procedimientos de Prueba del Enfoque Definido** **11.3.2.a** Evalúe los informes de escaneo del ASV de los últimos 12 meses para verificar que se realizaron escaneos de vulnerabilidad externa al menos una vez cada tres meses en el período de 12 meses más reciente. **11.3.2.b** Evalúe los resultados de los informes de escaneo del ASV de cada escaneo y re-escaneo realizado en los últimos 12 meses, para verificar que las vulnerabilidades se han resuelto y que se cumplen los requisitos de la Guía del Programa ASV para aprobar el escaneo. **11.3.2.c** Evalúe los informes de escaneo ASV para verificar que los escaneos fueron realizados por un Proveedor de Escaneo Aprobado por PCI SSC (ASV).	**Objetivo** Habitualmente, los atacantes buscan servidores externos sin parches o vulnerables, que pueden ser aprovechados para lanzar un ataque dirigido. Las organizaciones deben asegurarse de que estos dispositivos de cara al exterior se escanean regularmente en busca de debilidades y que las vulnerabilidades se parchean o se remedian para proteger a la entidad. Debido a que las redes externas corren un mayor riesgo de verse comprometidas, el escaneo de vulnerabilidades externas debe realizarse al menos una vez cada tres meses por un Proveedor de Escaneo Aprobado por PCI SSC (ASV). **Buenas Prácticas** Si bien se requieren escaneos al menos una vez cada tres meses, se recomienda realizar escaneos más frecuentes según la complejidad de la red, la frecuencia de los cambios y los tipos de dispositivos, software y sistemas operativos utilizados. Se pueden combinar varios informes de escaneo para demostrar que se han escaneo todos los sistemas y que se han resuelto todas las vulnerabilidades aplicables como parte del ciclo de escaneo de vulnerabilidades de tres meses. Sin embargo, puede requerirse documentación adicional para verificar que las vulnerabilidades no remediadas están en proceso de ser resueltas.

Requisitos y Procedimientos de Prueba		Guía
Sin embargo, durante los años siguientes después de la evaluación inicial PCI DSS, deben haberse realizado escaneos aprobados al menos cada tres meses. Las herramientas de escaneo de ASV pueden escanear una amplia gama de tipos y topologías de redes. Cualquier detalle sobre el entorno de destino (por ejemplo, distribuidores de carga, proveedores externos, ISP, configuraciones específicas, protocolos en uso, interferencia de escaneo) debe resolverse entre el ASV y el cliente de escaneo. Consulte la *Guía del Programa ASV* publicada en el sitio web PCI SCC para conocer las responsabilidades del cliente de escaneo, la preparación del escaneo, etc.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** El escaneo de un entorno después de cualquier cambio significativo garantiza que los cambios se realizaron adecuadamente, de manera que la seguridad del entorno no se vio comprometida a causa del cambio. **Buenas Prácticas** Las entidades deben incluir la necesidad de realizar análisis después de cambios significativos como parte del proceso de cambio y antes de considerar el cambio como completo. Todos los componentes del sistema afectados por el cambio deberán ser escaneos.
11.3.2.1 Los escaneos externos se realizan después de cualquier cambio significativo de la siguiente manera: • Se resuelven las vulnerabilidades calificadas con 4.0 o más por CVSS. • Los re-escaneos se realizan según sea necesario. • Los escaneos son realizados por personal cualificado con la independencia organizacional del probador (no se requiere que sea un QSA o ASV).	**11.3.2.1.a** Evalúe la documentación de control de cambios y los informes de escaneo externos para verificar que los componentes del sistema fueron escaneos después de cualquier cambio significativo.	
	11.3.2.1.b Entreviste al personal y examine los informes de escaneo externo y re-escaneo para verificar que se realizaron escaneos externos después de cambios significativos y que las vulnerabilidades calificadas con 4.0 o más por el CVSS fueron resueltas.	
Objetivo del Enfoque Personalizado La postura de seguridad de todos los componentes del sistema se verifica tras la realización de cambios significativos en la red o en los sistemas, mediante el uso de herramientas diseñadas para detectar vulnerabilidades que operan desde fuera de la red. Las vulnerabilidades detectadas se evalúan y rectifican sobre la base de un marco formal de evaluación de riesgos.	**11.3.2.1.c** Entreviste al personal para verificar que los escaneos externos sean realizados por recursos internos calificados o por un tercero externo calificado y con la independencia organizacional del asesor.	

Requisitos y Procedimientos de Prueba		Guía
11.4 Las pruebas de penetración externas e internas se realizan con regularidad y se corrigen las vulnerabilidades explotables y las debilidades de seguridad.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
11.4.1 La entidad define, documenta e implementa una metodología de prueba de penetración, que incluye: • Enfoques de pruebas de penetración aceptados por la industria. • Cobertura para todo el perímetro de CDE y sus sistemas críticos. • Pruebas tanto dentro como fuera de la red. • Pruebas para validar cualquier control de segmentación y reducción del alcance. • Pruebas de penetración a nivel de la aplicación para identificar, como mínimo, las vulnerabilidades enumeradas en el Requisito 6.2.4. • Las pruebas de penetración a nivel de red que abarcan todos los componentes que admiten las funciones de red y los sistemas operativos. • Revisión y consideración de amenazas y vulnerabilidades experimentadas en los últimos 12 meses. • Enfoque documentado para evaluar y abordar el riesgo que plantean las vulnerabilidades explotables y las debilidades de seguridad encontradas durante las pruebas de penetración. Retención de los resultados de las pruebas de penetración y los resultados de las actividades de remediación durante al menos 12 meses. *(continúa en la página siguiente)*	**11.4.1** Evalúe la documentación y entreviste al personal para verificar que la metodología de prueba de penetración definida, documentada e implementada por la entidad incluye todos los elementos especificados en este requisito.	**Objetivo** Los atacantes pasan mucho tiempo buscando vulnerabilidades externas e internas que aprovechar para obtener acceso a los datos de los titulares de tarjetas y luego exfiltrarlos. Como tal, las entidades necesitan probar sus redes detalladamente, tal como lo haría un atacante. Esta prueba permite a la entidad identificar y remediar las debilidades que podrían aprovecharse para comprometer la red y los datos de la entidad, y luego tomar las acciones apropiadas para proteger la red y los componentes del sistema de tales ataques. **Buenas Prácticas** Las técnicas de pruebas de penetración diferirán según las necesidades y la estructura de una organización, y deberían ser adecuadas para el entorno probado; por ejemplo, las pruebas de *fuzzing*, inyección y falsificación podrían ser apropiadas. El tipo, la profundidad y la complejidad de las pruebas dependerán del entorno específico y de las necesidades de la organización. **Definiciones** Las pruebas de penetración simulan una situación de ataque del mundo real con la intención de identificar hasta qué punto un atacante podría penetrar en un entorno, dadas las diferentes cantidades de información proporcionada al asesor. Esto permite a la entidad mayor comprensión de su exposición potencial y cómo desarrollar una estrategia para defenderse de los ataques. Una prueba de penetración difiere de un escaneo de vulnerabilidades, ya que una prueba de penetración es un proceso activo que generalmente incluye la explotación de las vulnerabilidades identificadas.

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Se define una metodología formal para pruebas técnicas exhaustivas que intentan explotar vulnerabilidades y debilidades de seguridad a través de métodos de ataque simulados por un atacante manual competente.		El escaneo en busca de vulnerabilidades por sí solo no es una prueba de penetración, ni una prueba de penetración adecuada si la atención se centra únicamente en tratar de aprovechar las vulnerabilidades encontradas en un escaneo de vulnerabilidades. Realizar un escaneo de vulnerabilidades puede ser uno de los primeros pasos, pero no es el único paso que realizará un asesor de penetración para planificar la estrategia de prueba. Incluso si un escaneo de vulnerabilidades no detecta vulnerabilidades conocidas, el asesor de penetración a menudo obtendrá suficiente conocimiento sobre el sistema como para identificar posibles brechas de seguridad. La prueba de penetración es un proceso muy manual. Si bien se pueden usar algunas herramientas automatizadas, el asesor aplica su conocimiento de los sistemas para obtener acceso a un entorno. A menudo, el asesor encadenará varios tipos de vulnerabilidades con el objetivo de atravesar las capas de defensa. Por ejemplo, si el asesor encuentra una manera de obtener acceso a un servidor de aplicaciones, el asesor utilizará el servidor comprometido como punto para organizar un nuevo ataque basado en los recursos a los que tiene acceso el servidor. De esta manera, un asesor puede simular las técnicas utilizadas por un atacante para identificar áreas de potencial debilidad en el entorno. También se debe considerar la prueba de métodos de detección y monitoreo de seguridad, por ejemplo, para confirmar la efectividad de los mecanismos de monitoreo de integridad de archivos y registro. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Realizar pruebas desde el interior de la red (o "pruebas de penetración interna") significa realizar pruebas tanto desde el interior del CDE como hacia el CDE proviniendo de redes internas confiables y no confiables. Pruebas desde fuera de la red (o pruebas de penetración "externas") significa probar el perímetro externo expuesto de redes confiables y sistemas críticos conectado o accesible a infraestructuras de redes públicas.		**Información Adicional** Refiérase a la *Información Complementaria: Guía de Pruebas de Penetración* para orientación adicional. Los enfoques de pruebas de penetración aceptados por la industria incluyen: *Manual y Metodología de las Pruebas de Seguridad de Código Abierto (OSSTMM)* *Programas de Pruebas de Penetración Open Web Application Security Project (OWASP).*

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.4.2 Se realizan pruebas de penetración interna: • Según la metodología definida por la entidad, • Al menos una vez cada 12 meses. • Después de cualquier actualización o cambio significativo de infraestructura o aplicación • Por un recurso interno calificado o un tercero externo calificado • El asesor cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).	**11.4.2.a** Evalúe el alcance del trabajo y los resultados de la prueba de penetración interna más reciente para verificar que la prueba de penetración se realice de acuerdo con todos los elementos especificados en este requisito. **11.4.2.b** Entreviste al personal para verificar que la prueba de penetración interna fue realizada por un recurso interno calificado o un tercero externo calificado y con la independencia organizacional del asesor (no es necesario que sea un QSA o ASV).	Las pruebas de penetración interna tienen dos propósitos. En primer lugar, al igual que una prueba de penetración externa, descubre vulnerabilidades y configuraciones incorrectas que podrían ser utilizadas por un atacante que hubiese logrado obtener cierto grado de acceso a la red interna, ya sea porque el atacante es un usuario autorizado que realiza actividades no autorizadas o un atacante externo que había logrado penetrar el perímetro de la entidad. En segundo lugar, las pruebas de penetración internas también ayudan a las entidades a descubrir dónde falló su proceso de control de cambios al detectar sistemas previamente desconocidos. Además, verifica el estado de muchos de los controles que operan dentro del CDE. Una prueba de penetración no es realmente una "prueba" porque el resultado de una prueba de penetración no es algo que pueda clasificarse como "aprobado" o "reprobado". El mejor resultado de una prueba es un catálogo de vulnerabilidades y configuraciones erróneas que la entidad no conocía y que el asesor de penetración encontró antes que un atacante. Una prueba de penetración que no encontró nada es típicamente indicativa de faltas del asesor de penetración, en lugar de ser un reflejo positivo de la postura de seguridad de la entidad. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado		
Las defensas internas del sistema se verifican mediante pruebas técnicas de acuerdo con la metodología definida por la entidad con la frecuencia necesaria para abordar los ataques y amenazas nuevos y en evolución, y para garantizar que los cambios significativos no introduzcan vulnerabilidades desconocidas.		

Requisitos y Procedimientos de Prueba		Guía
		Buenas Prácticas Algunas consideraciones a tomar en cuenta cuando se está escogiendo recursos calificados para realizar pruebas de penetración incluyen: • Certificaciones de pruebas de penetración específicas, que pueden ser una indicación del nivel de habilidad y competencia del asesor. • La experiencia previa en la realización de pruebas de penetración, por ejemplo, cuántos de años de experiencia y el tipo y alcance de compromisos anteriores pueden ayudar a confirmar si la experiencia del asesor es adecuada para las necesidades del compromiso. **Información Adicional** • Refiérase a la *Información Complementaria: Guía de Pruebas de Penetración* en el sitio web PCI SCC para obtener orientación adicional.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
11.4.3 Se realizan pruebas de penetración externa: • Según la metodología definida por la entidad • Al menos una vez cada 12 meses • Después de cualquier actualización o cambio significativo de infraestructura o aplicación • Por un recurso interno calificado o un tercero externo calificado • El asesor cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).	**11.4.3.a** Evalúe el alcance del trabajo y los resultados de la prueba de penetración externa más reciente para verificar que la prueba de penetración se realice de acuerdo con todos los elementos especificados en este requisito.	
	11.4.3.b Entreviste al personal para verificar que la prueba de penetración externa fue realizada por un recurso interno calificado o un tercero externo calificado y que existe independencia organizacional del asesor (no se requiere que sea un QSA o ASV).	
Objetivo del Enfoque Personalizado		
Las defensas del sistema externo se verifican mediante pruebas técnicas de acuerdo con la metodología definida por la entidad con la frecuencia necesaria para abordar los ataques y amenazas nuevos y en evolución, y para garantizar que los cambios significativos no introduzcan vulnerabilidades desconocidas.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Los resultados de una prueba de penetración suelen ser una lista priorizada de vulnerabilidades descubiertas por el ejercicio. A menudo, un asesor habrá encadenado una serie de vulnerabilidades para comprometer un componente del sistema. La reparación de las vulnerabilidades encontradas mediante una prueba de penetración reduce significativamente la probabilidad de que un atacante malintencionado explote las mismas vulnerabilidades. Utilizando el propio proceso de evaluación de riesgos de vulnerabilidad de la entidad (consulte el requisito 6.3.1) garantiza que las vulnerabilidades que representan el mayor riesgo para la entidad se remediarán más rápidamente. **Buenas Prácticas** Como parte de la evaluación del riesgo de la entidad, las entidades deben considerar qué tan probable es que se explote la vulnerabilidad y si existen otros controles presentes en el entorno para reducir el riesgo. Se debe abordar cualquier debilidad que indique que no se cumplen los requisitos de PCI DSS.
11.4.4 Las vulnerabilidades explotables y las debilidades de seguridad encontradas durante las pruebas de penetración se corrigen de la siguiente manera: • De acuerdo con la evaluación de la entidad, del riesgo que representa el problema de seguridad según se define en el Requisito 6.3.1. • La prueba de penetración se repite para verificar las correcciones.	**11.4.4** Evalúe los resultados de las pruebas de penetración para verificar que las vulnerabilidades explotables y las debilidades de seguridad observadas se corrigieron de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado		
Las vulnerabilidades y las debilidades de seguridad encontradas al verificar que se mitigan las defensas del sistema.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.4.5 Si la segmentación se utiliza para aislar el CDE de otras redes, las pruebas de penetración se realizan en los controles de segmentación de la siguiente manera: • Al menos una vez cada 12 meses y después de cualquier cambio en los controles/métodos de segmentación. • Cubriendo todos los controles/métodos de segmentación en uso. • De acuerdo con la metodología de prueba de penetración definida por la entidad. • Confirmar que los controles/métodos de segmentación son operativos y eficientes, y aislar al CDE de todos los sistemas fuera del ámbito. • Confirmar la efectividad de cualquier uso de aislamiento para separar sistemas con diferentes niveles de seguridad (ver Requisito 2.2.3). • Realizado por un recurso interno calificado o un tercero externo calificado. • El asesor cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).	**11.4.5.a** Evalúe los controles de segmentación y revisar la metodología de prueba de penetración para verificar que los procedimientos de prueba de penetración estén definidos para probar todos los métodos de segmentación de acuerdo con todos los elementos especificados en este requisito. **11.4.5.b** Evalúe los resultados de las pruebas de penetración más recientes para verificar que cubra y aborde todos los elementos especificados en este requisito. **11.4.5.c** Entreviste al personal para verificar que la prueba fue realizada por un recurso interno calificado o un tercero externo calificado y que existe independencia organizacional del asesor (no se requiere que sea un QSA o ASV).	Cuando una entidad utiliza controles de segmentación para aislar el CDE de las redes internas que no son de confianza, la seguridad del CDE depende del funcionamiento de esa segmentación. Muchos ataques han involucrado a un atacante moviéndose lateralmente desde lo que una entidad consideraba una red aislada hacia el CDE. El uso de técnicas y herramientas de prueba de penetración para validar que una red que no es de confianza está de hecho aislada del CDE, puede alertar a la entidad sobre una falla o mala configuración de los controles de segmentación, que luego pueden rectificarse. **Buenas Prácticas** Se pueden utilizar técnicas como el descubrimiento de host y el escaneo de puertos para verificar que los segmentos fuera del alcance no tengan acceso al CDE.
Objetivo del Enfoque Personalizado		
Si se utiliza la segmentación, se verifica periódicamente mediante pruebas técnicas que sea continuamente eficaz, incluso después de cualquier cambio, para aislar el CDE de todos los sistemas fuera del ámbito.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.4.6 ***Requisito Adicional Solo para Proveedores de Servicios:*** Si la segmentación se utiliza para aislar el CDE de otras redes, las pruebas de penetración se realizan en los controles de segmentación de la siguiente manera: • Al menos una vez cada seis meses y después de cualquier cambio en los controles/métodos de segmentación. • Cubriendo todos los controles/métodos de segmentación en uso. • De acuerdo con la metodología de prueba de penetración definida por la entidad. • Confirmar que los controles/métodos de segmentación son operativos y eficientes, y aislar al CDE de todos los sistemas fuera del ámbito. • Confirmar la efectividad de cualquier uso de aislamiento para separar sistemas con diferentes niveles de seguridad (ver Requisito 2.2.3). • Realizado por un recurso interno calificado o un tercero externo calificado. • El asesor cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).	**11.4.6.a** ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Evalúe los resultados de la prueba de penetración más reciente para verificar que la penetración cubra y aborde todos los elementos especificados en este requisito. **11.4.6.b** ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Entreviste al personal para verificar que la prueba fue realizada por un recurso interno calificado o un tercero externo calificado y que existe independencia organizacional del asesor (no se requiere que sea un QSA o ASV).	Típicamente los proveedores de servicios tienen acceso a mayores volúmenes de datos de titulares de tarjetas o pueden proporcionar un punto de entrada que se puede explotar para luego comprometer a muchas otras entidades. Los proveedores de servicios también suelen tener redes más amplias y complejas que están sujetas a cambios más frecuentes. La probabilidad de que fallen los controles de segmentación en redes complejas y dinámicas es mayor en entornos de proveedores de servicios. Es probable que la validación de los controles de segmentación con más frecuencia descubra tales fallas antes de que puedan ser explotadas por un atacante que intente pivotar lateralmente desde una red no confiable fuera del ámbito hacia el CDE. **Buenas Prácticas** Si bien el requisito especifica que esta validación del alcance se desarrolla como mínimo cada seis meses y después de un cambio significativo, este ejercicio debe realizarse con la mayor frecuencia posible para garantizar que siga siendo eficaz para aislar al CDE de otras redes.
Objetivo del Enfoque Personalizado Si se utiliza la segmentación, se verifica mediante pruebas técnicas que sea continuamente eficiente, incluso después de cualquier cambio, para aislar el CDE de los sistemas fuera del ámbito.		

(continúa en la página siguiente)

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios.		
Requisitos del Enfoque Definido **11.4.7** ***Requisito adicional sólo para los proveedores de servicios multi-arrendamiento***: *Los proveedores de servicios multi-arrendamiento apoyan a sus clientes para las pruebas de penetración externas según los Requisitos 11.4.3 y 11.4.4.* **Objetivo del Enfoque Personalizado** Los proveedores de servicios multi-arrendamiento apoyan las necesidades de sus clientes de realizar pruebas técnicas, ya sea proporcionando acceso o pruebas de que se han realizado pruebas técnicas comparables. *(continúa en la página siguiente)*	**Procedimientos de Prueba del Enfoque Definido** **11.4.7** ***Procedimiento de prueba adicional sólo para los proveedores de servicios multi-arrendamiento:*** Evalúe las pruebas para verificar que los proveedores de servicios multi-arrendamiento apoyan a sus clientes en las pruebas de penetración externas según los requisitos 11.4.3 y 11.4.4.	**Objetivo** Las entidades deben realizar pruebas de penetración de acuerdo con PCI DSS para simular el comportamiento de los atacantes y descubrir vulnerabilidades en su entorno. En entornos compartidos y en la nube, el proveedor de servicios de terceros puede estar preocupado por las actividades de un asesor de penetración que afecta los sistemas de otros clientes. Los proveedores de servicios multi-arrendamiento no pueden prohibir las pruebas de penetración porque esto dejaría los sistemas de sus clientes abiertos a la explotación. Por lo tanto, los proveedores de servicios multi-arrendamiento deben apoyar las solicitudes de los clientes para llevar a cabo pruebas de penetración o para los resultados de las pruebas de penetración.

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito sólo se aplica cuando la entidad evaluada es un proveedor de servicios multi-arrendamiento. Para cumplir con este requisito, un proveedor de servicios multi-arrendamiento puede: • Proporcionar evidencia a sus clientes para demostrar que se han realizado pruebas de penetración de acuerdo con los Requisitos 11.4.3 y 11.4.4 en la infraestructura suscrita por los clientes, o • Brindar acceso rápido a cada uno de sus clientes para que puedan realizar sus propias pruebas de penetración. La evidencia proporcionada a los clientes puede incluir resultados de pruebas de penetración redactados, pero debe incluir información suficiente para demostrar que todos los elementos de los Requisitos 11.4.3 y 11.4.4 se han cumplido en nombre del cliente. *Consulte también el Anexo A1: Requisitos Adicionales PCI DSS para Proveedores de Servicios Multi-Arrendamiento.* *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
11.5 Las intrusiones de red y los cambios inesperados de archivos se detectan y se responden.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
11.5.1 Las técnicas de detección y/o prevención de intrusiones se utilizan para detectar y/o impedir intrusiones en la red de la siguiente manera: • Todo el tráfico se supervisa en el perímetro del CDE. • Todo el tráfico se supervisa en los puntos críticos del CDE. • Se envía una alerta al personal indicando las sospechas de situaciones comprometidas. • Todos los motores de detección y prevención de intrusiones, las líneas de base y las firmas se mantienen actualizadas.	**11.5.1.a** Evalúe las configuraciones del sistema y los diagramas de la red para verificar que las técnicas de detección y/o prevención de intrusos están implementadas para monitorear todo el tráfico: • En el perímetro del CDE. • En los puntos críticos del CDE.	**Objetivo** Las técnicas de detección y/o prevención de intrusiones (como los IDS/IPS) comparan el tráfico que llega a la red con "firmas" conocidas y/o comportamientos de miles de tipos de situaciones comprometidas (herramientas de hackers, troyanos y otros programas maliciosos), y luego envían alertas y/o detienen el intento a medida que se produce. Sin un enfoque proactivo para detectar la actividad no autorizada, los ataques a los recursos informáticos (o su uso indebido) podrían pasar desapercibidos durante largos periodos de tiempo. El impacto de una intrusión en el CDE es, en muchos sentidos, un factor del tiempo que un atacante tiene en el entorno antes de ser detectado. **Buenas Prácticas** Las alertas de seguridad generadas por estas técnicas deben ser supervisadas continuamente para detener los intentos de intrusión o las intrusiones reales, y limitar los daños potenciales. **Definiciones** Los lugares críticos podrían incluir, pero no se limitan a, los controles de seguridad de la red entre los segmentos de la red (por ejemplo, entre una DMZ y una red interna o entre una red dentro y fuera del ámbito de aplicación) y los puntos que protegen las conexiones entre un componente del sistema menos confiable y otro más confiable.
	11.5.1.b Evalúe las configuraciones de los sistemas y entreviste al personal responsable para comprobar que las técnicas de detección y/o prevención de intrusiones alertan al personal de los posibles riesgos.	
Objetivo del Enfoque Personalizado	**11.5.1.c** Evalúe las configuraciones del sistema y la documentación del proveedor para verificar que las técnicas de detección y/o prevención de intrusiones están configuradas para mantener actualizados todos los motores, bases de referencia y firmas.	
Se implementan mecanismos para detectar en tiempo real el tráfico de red sospechoso o anómalo que pueda ser indicativo de la actividad de los actores de la amenaza. Las alertas generadas por estos mecanismos son respondidas por el personal, o por medios automatizados que aseguran que los componentes del sistema no estarán en una situación comprometida como resultado de la actividad detectada.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
11.5.1.1 ***Requisito adicional sólo para proveedores de servicios:*** Las técnicas de detección-intrusión y/o intrusión-prevención detectan, alertan/impiden y abordan los canales de comunicación de malware encubierto.	**11.5.1.1.a** ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Evalúe la documentación y los ajustes de configuración para verificar que los métodos para detectar y alertar/evitar los canales de comunicación de malware encubierto están instalados y funcionando.	**Objetivo** La detección de intentos de comunicación de malware encubierto (por ejemplo, *tunelización* de DNS) puede ayudar a bloquear la propagación de malware lateralmente dentro de una red y la *exfiltración* de datos. A la hora de decidir dónde colocar este control, las entidades deben tener en cuenta las ubicaciones críticas de la red y las rutas probables de los canales encubiertos. Cuando el malware se afianza en un entorno infectado, suele intentar establecer un canal de comunicación con un servidor de mando y control (C&C). A través del servidor de C&C, el atacante se comunica y controla el malware en los sistemas comprometidos para entregar cargas maliciosas o instrucciones maliciosas, o para iniciar la *exfiltración* de datos. En muchos casos, el malware se comunicará con el servidor de C&C de forma indirecta a través de robots informáticos, eludiendo la vigilancia, los controles de bloqueo y haciendo que estos métodos sean ineficientes para detectar los canales encubiertos. **Buenas Prácticas** Los métodos que pueden ayudar a detectar y abordar los canales de comunicación del malware incluyen el escaneo de puntos finales en tiempo real, el filtrado del tráfico de salida, una lista de "permitidos", herramientas de prevención de pérdida de datos y herramientas de supervisión de la seguridad de la red, como IDS/IPS. Además, las consultas y respuestas de DNS son una fuente de datos esencial utilizada por los defensores de la red para apoyar la respuesta a incidentes, así como el descubrimiento de intrusiones. Cuando estas transacciones se recogen para su procesamiento y análisis, pueden permitir una serie de valiosos escenarios de análisis de seguridad.
	11.5.1.1.b ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Evalúe el plan de respuesta a incidentes de la entidad (requisito 12.10.1) para comprobar que exige y define una respuesta en caso de que se detecten canales de comunicación de malware encubiertos.	
	11.5.1.1.c ***Procedimiento de prueba adicional sólo para las evaluaciones de los proveedores de servicios:*** Entreviste al personal responsable y observe los procesos para verificar que el personal conoce las técnicas de comunicación y control de malware encubierto y sabe cómo responder cuando hay sospechas de malware.	
Objetivo del Enfoque Personalizado		
Existen mecanismos para detectar y alertar/impedir las comunicaciones encubiertas con los sistemas de mando y control. Las alertas generadas por estos mecanismos son respondidas por el personal, o por medios automatizados que garantizan el bloqueo de dichas comunicaciones.		

(continúa en la página siguiente)

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		Es importante que las organizaciones mantengan un conocimiento actualizado de los modos de operación del malware, ya que mitigarlos puede ayudar a detectar y limitar el impacto del malware en el entorno.
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Los cambios en los archivos críticos del sistema, la configuración o el contenido pueden ser un indicador de que un atacante ha ingresado al sistema de la organización. Dichos cambios pueden permitir a un atacante realizar acciones maliciosas adicionales, ingresar a los datos de los titulares de las tarjetas y/o llevar a cabo actividades sin ser detectadas o registradas. *(continúa en la página siguiente)*
11.5.2 Un mecanismo de detección de cambios (por ejemplo, herramientas de monitoreo de integridad de archivos) se despliega como sigue: • Para alertar al personal sobre modificaciones no autorizadas (incluyendo cambios, adiciones y eliminaciones) de archivos críticos. • Para realizar comparaciones de archivos críticos al menos una vez por semana.	**11.5.2.a** Evalúe la configuración del sistema, los archivos monitoreados y los resultados de las actividades de monitoreo para verificar el uso de un mecanismo de detección de cambios. **11.5.2.b** Evalúe las configuraciones del mecanismo de detección de cambios para verificar que está configurado de acuerdo con todos los elementos especificados en este requisito.	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Los archivos críticos no pueden ser modificados por personal no autorizado sin que se genere una alerta.		Un mecanismo de detección de cambios detectará y evaluará dichos cambios en los archivos críticos y generará alertas a las que se puede responder siguiendo procesos definidos para que el personal pueda tomar las medidas adecuadas. Si el resultado de la solución de detección de cambios no se implementa correctamente y es monitoreado, individuos malintencionados podrían añadir, eliminar o alterar el contenido de los archivos de configuración, los programas del sistema operativo o los ejecutables de las aplicaciones. Si no se detectan los cambios no autorizados, esto podría dejar sin efecto los controles de seguridad existentes y/o provocar el robo de los datos de titulares de tarjetas sin un impacto perceptible en el procesamiento normal. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad A efectos de detección de cambios, los archivos críticos suelen ser aquellos que no cambian regularmente, pero cuya modificación podría indicar poner en riesgo el sistema o comprometerlo. Los mecanismos de detección de cambios, como los productos de monitoreo de la integridad de los archivos, suelen venir pre-configurados con archivos críticos para el sistema operativo correspondiente. Otros archivos críticos, como los de las aplicaciones personalizadas, deben ser evaluados y definidos por la entidad (es decir, el comerciante o proveedor de servicios).		**Buenas Prácticas** Algunos ejemplos de los tipos de archivos que deben ser supervisados incluyen, pero no se limitan a: • Los ejecutables del sistema. • Archivos ejecutables de la aplicación. • Archivos de configuración y parámetros. • Registros de auditoría almacenados centralmente, históricos o archivados. • Archivos críticos adicionales determinados por la entidad (por ejemplo, a través de la evaluación de riesgos u otros medios). **Ejemplos** Las soluciones de detección de cambios, como las herramientas de supervisión de la integridad de los archivos (FIM), comprueban los cambios, las adiciones y las supresiones en los archivos críticos, y notifican cuando se detectan dichos cambios.

Requisitos y Procedimientos de Prueba		Guía
11.6 Se detectan los cambios no autorizados en las páginas de pago se detectan y se responden.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
11.6.1 El mecanismo de detección de cambios y manipulaciones se despliega de la siguiente manera: • Para enviar alertas al personal sobre modificaciones no autorizadas (incluyendo indicadores de situaciones comprometidas, cambios, adiciones y supresiones) en los encabezados HTTP y en el contenido de las páginas de pago tal y como las recibe el navegador del consumidor. • El mecanismo está configurado para evaluar el encabezamiento HTTP y la página de pago recibidas. • Las funciones del mecanismo se realizan de la siguiente manera: – Al menos una vez cada siete días **O** – Periódicamente, (a una frecuencia definida en el análisis de riesgos específico de la entidad, el cual se desarrolla de acuerdo a todos los elementos especificados en el Requisito 12.3.1.)	**11.6.1.a** Evalúe la configuración del sistema, las páginas de pago monitoreadas y los resultados de las actividades de monitoreo para verificar el uso de un mecanismo de detección de cambios y alteraciones. **11.6.1.b** Evalúe los parámetros de configuración para verificar que el mecanismo esté configurado de acuerdo con todos los elementos especificados en este requisito. **11.6.1.c** Si las funciones del mecanismo se desempeñan con una frecuencia definida por la entidad, evalúe el análisis de riesgo específico de la entidad para determinar la frecuencia a fin de verificar que el análisis de riesgo se realizó de acuerdo con todos los elementos especificados en el Requisito 12.3 .1. **11.6.1.d** Evalúe los ajustes de configuración y entreviste al personal para verificar que las funciones del mecanismo se realicen: • Al menos una vez cada siete días **O** • Con la frecuencia definida en el análisis de riesgo específico de la entidad realizado para este requisito.	Muchas páginas web se basan ahora en el ensamblaje de objetos, incluyendo el contenido activo (principalmente JavaScript), desde múltiples ubicaciones de Internet. Además, el contenido de muchas páginas web se define utilizando sistemas de gestión de contenidos y de etiquetas que podrían no ser monitoreadas utilizando mecanismos tradicionales de detección de cambios. Por lo tanto, el único lugar para detectar cambios o indicadores de actividad maliciosa es en el navegador del consumidor mientras se construye la página y se interpreta todo el JavaScript. Comparando la versión actual del encabezado HTTP y el contenido activo de las páginas de pago que recibe el navegador del consumidor con versiones anteriores o conocidas, es posible detectar cambios no autorizados que puedan indicar un ataque de *skimming.* Además, al buscar indicadores conocidos de amenazas y elementos de script o comportamientos típicos de los ladrones de información, se pueden levantar alertas sospechosas.
Objetivo del Enfoque Personalizado		
El código de *E-commerce* de *skimming* o las técnicas no pueden ser agregados a las páginas de pago recibidas por el navegador del consumidor sin que se genere una alerta oportuna. Las medidas *anti-skimming* no se pueden eliminar de las páginas de pago sin que se genere una alerta rápida.		

(continúa en la página siguiente)

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad La intención de este requisito no es que una entidad necesite instalar software en los sistemas o navegadores de sus consumidores, sino que la entidad utilice técnicas como las descritas en los ejemplos anteriores para detectar e impedir actividades inesperadas de *scripts.* *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		**Ejemplos** Los mecanismos que detectan y reportan los cambios en los encabezados y el contenido de las páginas de pago incluyen, entre otros: • Las Infracciones de la Política de Seguridad de Contenido (CSP) se pueden reportar a la entidad mediante las directivas *CSP report-to o report-uri.* • Los cambios en el CSP en sí pueden indicar una manipulación. • El monitoreo externo por parte de los sistemas que solicitan y analizan las páginas web recibidas (también conocido como monitoreo sintético de usuarios) puede detectar cambios en JavaScript en las páginas de pago y alertar al personal. • La incrustación de un script de detección de alteraciones a prueba de manipulaciones en la página de pago puede alertar y bloquear cuando se detecta un comportamiento de script malicioso. • Los *proxies* inversos y las Redes de Entrega de Contenido pueden detectar cambios en los scripts y alertar al personal. A menudo, estos mecanismos se basan en una suscripción o en la nube, pero también pueden basarse en soluciones personalizadas.

Mantener una Política de Protección Informática

Requisito 12: Respaldar la Seguridad de la Información con Políticas y Programas Organizacionales

Secciones	
12.1	Una política integral de seguridad de la información, que rija y proporcione orientación para la protección de los activos de información de la entidad, es actualizada y bien conocida.
12.2	Se definen e implementan políticas de uso aceptable para las tecnologías orientadas al usuario final.
12.3	Los riesgos para el entorno de datos de titulares de tarjetas se identifican, evalúan y gestionan formalmente.
12.4	Gestión del cumplimiento con PCI DSS.
12.5	Documentación y validación del alcance PCI DSS.
12.6	La educación en concienciación sobre la seguridad es una actividad continua.
12.7	El personal es evaluado para reducir los riesgos de las amenazas internas.
12.8	Gestión del riesgo para los activos de información asociados a las relaciones con proveedores de servicios de terceros (TPSP).
12.9	Los proveedores de servicios de terceros (TPSP) respaldan el cumplimiento de sus clientes con PCI DSS.
12.10	Respuesta inmediata a incidentes de seguridad sospechosos y confirmados que podrían afectar al CDE.

Descripción

La política general de seguridad de la información de la organización marca la pauta para toda la entidad e informa al personal lo que se espera de ellos. Todo el personal debe ser consciente de la sensibilidad de los datos de los titulares de tarjetas y de sus responsabilidades para protegerlos.

Para propósitos del Requisito 12, "personal" se refiere a los empleados de tiempo completo y parcial, empleados temporales, contratistas y consultores con responsabilidades de seguridad para proteger los datos de cuenta o que puedan afectar la seguridad de los datos de cuentas.

Consulte el Anexo G para acceder a las definiciones de los términos PCI DSS.

Requisitos y Procedimientos de Prueba		Guía
12.1 Una política integral de seguridad de la información que rija y proporcione orientación para la protección de los activos de información de la entidad es actualizada y bien conocida.		
Requisitos del Enfoque Definido **12.1.1** Una política general de seguridad de la información es: • Establecida. • Publicada. • Mantenida. • Difundida a todo el personal relevante, así como a los proveedores y socios de negocios relevantes. **Objetivo del Enfoque Personalizado** Los objetivos estratégicos y los principios de seguridad de la información son definidos, adoptados y conocidos por todo el personal.	**Procedimientos de Prueba del Enfoque Definido** **12.1.1** Evalúe las políticas de uso aceptable de las tecnologías de usuario final y entreviste al personal responsable para comprobar que los procesos están documentados y se aplican de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** La política general de seguridad de la información de una organización se vincula con y rige a todas las demás políticas y procedimientos que definen la protección de los datos de titulares de tarjetas. La política de seguridad de la información comunica la intención y los objetivos de la administración con respecto a la protección de sus activos más valiosos, incluidos los datos de titulares de tarjetas. Sin una política de seguridad de la información, las personas tomarán sus propias decisiones sobre los controles que se requieren dentro de la organización, lo que puede hacer que la organización no cumpla con sus obligaciones legales, reglamentarias y contractuales, ni pueda proteger adecuadamente sus activos de manera consistente. Para garantizar que las políticas sean implementadas, es importante que todo el personal relevante dentro de la organización, así como los terceros, proveedores y socios de negocios relevantes, conozcan las políticas de seguridad de la información de la organización y sus responsabilidades para proteger los activos de información. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
		Buenas Prácticas La política de seguridad de la organización identifica el propósito, el alcance, la responsabilidad y la información que define claramente la posición de la organización con respecto a la seguridad de la información. La política general de seguridad de la información difiere de las políticas de seguridad individuales que abordan tecnologías o disciplinas de seguridad específicas. Esta política establece las directivas para toda la organización, mientras que las políticas de seguridad individuales alinean y respaldan la política de seguridad general y comunican objetivos específicos para la tecnología o disciplinas de seguridad. Es importante que todo el personal relevante dentro de la organización, así como los terceros, proveedores y socios de negocios relevantes, conozcan la política de seguridad de la información de la organización y sus responsabilidades para proteger los activos de información. **Definiciones** “Relevante” para este requisito significa que la política de seguridad de la información se difunde a aquellos con roles aplicables a algunos o todos los temas de la política, ya sea dentro de la empresa o debido a servicios/funciones realizadas por un proveedor o un tercero.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **12.1.2** La política de seguridad de la información es: • Revisada al menos una vez cada 12 meses. • Actualizada según sea necesario para reflejar los cambios en los objetivos de negocios o los riesgos para el entorno. **Objetivo del Enfoque Personalizado** La política de seguridad de la información sigue reflejando los principios y objetivos estratégicos de la organización.	**Procedimientos de Prueba del Enfoque Definido** **12.1.2** Evalúe la política de seguridad de la información y entreviste al personal responsable para verificar que la política se administre de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Las amenazas a la seguridad y los métodos de protección asociados evolucionan rápidamente. Si no se actualiza la política de seguridad de la información para reflejar los cambios relevantes, es posible que no se aborden las nuevas medidas para defenderse de estas amenazas.
Requisitos del Enfoque Definido **12.1.3** La política de seguridad define claramente los roles y responsabilidades de seguridad de la información para todo el personal, y todo el personal conoce y reconoce sus responsabilidades en materia de seguridad de la información. **Objetivo del Enfoque Personalizado** El personal comprende su papel en la protección de los datos de titulares de tarjetas de la entidad.	**Procedimientos de Prueba del Enfoque Definido** **12.1.3.a** Evalúe las políticas de seguridad de la información para verificar que definan claramente los roles y responsabilidades de seguridad de la información para todo el personal. **12.1.3.b** Entrevistar al personal en varias funciones para verificar que comprenden sus responsabilidades en materia de seguridad de la información. **12.1.3.c** Evalúela evidencia documentada para verificar que el personal reconozca sus responsabilidades en materia de seguridad de la información.	**Objetivo** Sin roles y responsabilidades de seguridad claramente definidos y asignados, podría darse un mal uso de los activos de información de la organización o una interacción inconsistente con el personal de seguridad de la información, lo que podría llevar a una implementación insegura de tecnologías o al uso de tecnologías obsoletas o inseguras.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	
12.1.4 La responsabilidad de la seguridad de la información se asigna formalmente a un director de seguridad de la información o a otro miembro de la dirección ejecutiva con conocimientos de seguridad de la información.	**12.1.4** Evalúe las políticas de seguridad de la información para verificar que esté asignada formalmente a un Director de Seguridad de la Información o a otro miembro de la dirección ejecutiva con conocimientos de seguridad de la información.	**Objetivo** Para garantizar que alguien con suficiente autoridad y responsabilidad esté administrando y defendiendo activamente el programa de seguridad de la información de la organización, la responsabilidad y la rendición de cuentas por la seguridad de la información deben asignarse a nivel ejecutivo dentro de una organización. Los títulos de gestión ejecutiva comunes para esta función incluyen: director seguridad de la información, del inglés *Chief Information Security Officer* (CISO) y director de seguridad, del inglés *Chief Security Officer* (CSO); para cumplir con este requisito, la función de CSO debe ser responsable por la seguridad de la información). Estos puestos a menudo se ubican en el nivel más alto de la administración y forman parte del nivel de director ejecutivo o de nivel C, por lo general reportan al director ejecutivo o a la junta directiva. **Buenas Prácticas** Las entidades también deben considerar planes de transición y/o sucesión para este tipo de personal clave a fin de evitar posibles brechas en las actividades críticas de seguridad.
Objetivo del Enfoque Personalizado		
Un miembro designado de la dirección ejecutiva es responsable de la seguridad de la información.		

Requisitos y Procedimientos de Prueba		Guía
12.2 Se definen e implementan políticas de uso aceptable para tecnologías de usuario final.		
Requisitos del Enfoque Definido **12.2.1** Se documentan e implementan políticas de uso aceptable para tecnologías orientadas al usuario final, que incluyen: • Aprobación explícita por las partes autorizadas. • Usos aceptables de la tecnología. • Lista de productos aprobados por la empresa para uso de los empleados, incluidos hardware y software. **Objetivo del Enfoque Personalizado** El uso de tecnologías orientadas al usuario final es definido y gestionado para garantizar su uso autorizado. **Notas de Aplicabilidad** Ejemplos de tecnologías orientadas al usuario final para las que se espera sean aplicadas políticas de uso aceptable son, entre otras, tecnologías inalámbricas y de acceso remoto, computadoras portátiles, tabletas, teléfonos móviles y medios electrónicos extraíbles, uso del correo electrónico y uso de Internet.	**Procedimientos de Prueba del Enfoque Definido** **12.2.1** Evalúe las políticas de uso aceptable para las tecnologías de usuario final y entreviste al personal responsable para verificar que los procesos estén documentados e implementados de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Las tecnologías orientadas al usuario final son una inversión significativa y pueden representar un riesgo significativo para la organización si no se administran adecuadamente. Las políticas de uso aceptable describen el comportamiento esperado del personal cuando utiliza tecnologías informáticas pertenecientes a la organización y reflejan la tolerancia al riesgo de la organización. Estas políticas instruyen al personal sobre lo que pueden y no pueden hacer con equipos de la empresa e instruyen al personal sobre los usos correctos e incorrectos de los recursos de Internet y correo electrónico de la empresa. Dichas políticas pueden proteger legalmente a una organización y permitirle actuar cuando se violan las políticas. **Buenas Prácticas** Es importante que las políticas de uso estén respaldadas por controles técnicos para gestionar la aplicación de las políticas La estructuración de políticas como simples requisitos de "hacer" y "no hacer" que estén vinculados a un propósito puede ayudar a eliminar la ambigüedad y proporcionar al personal el contexto del requisito.

Requisitos y Procedimientos de Prueba		Guía
12.3 Los riesgos para el entorno de datos de titulares de tarjetas se identifican, evalúan y gestionan formalmente.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
12.3.1 Cada requisito de PCI DSS que proporciona flexibilidad sobre la frecuencia con la que se realizan (por ejemplo, los requisitos que deben realizarse periódicamente) está respaldado por un análisis de riesgo específico que está documentado e incluye: • Identificación de los activos a proteger. • Identificación de las amenazas contra las que protege el requisito. • Identificación de factores que contribuyen a la probabilidad y/o impacto de que se materialice una amenaza. • Análisis resultante que determine e incluya la justificación de la frecuencia con la que se debe realizar el requisito para minimizar la probabilidad de que se materialice la amenaza. • Revisión de cada análisis de riesgo específico al menos una vez cada 12 meses para determinar si los resultados siguen siendo válidos o si se necesita un análisis de riesgo actualizado. • Realización de análisis de riesgos actualizados cuando sea necesario, según lo determinado por la revisión anual.	**12.3.1** Evalúe las políticas y los procedimientos documentados para verificar que un proceso esté definido para realizar análisis de riesgo específicos para cada requisito de PCI DSS que brinde flexibilidad sobre la frecuencia con la que se realiza el requisito y que el proceso incluya todos los elementos especificados en este requisito.	Algunos requisitos de PCI DSS permiten que una entidad defina la frecuencia con la que se realiza una actividad en función del riesgo para su entorno. La realización de este análisis de riesgos de acuerdo con una metodología asegura la validez y coherencia con las políticas y procedimientos. Este análisis de riesgo dirigido (a diferencia de la evaluación de riesgo tradicional de toda la empresa) se centra en los requisitos de PCI DSS que permiten a una entidad flexibilidad sobre la frecuencia con la que una entidad realiza un control determinado. Para este análisis de riesgo, la entidad evalúa cuidadosamente cada requisito de PCI DSS que proporcionan esta flexibilidad y determina la frecuencia que respalda la seguridad adecuada para la entidad, y el nivel de riesgo que la entidad está dispuesta a aceptar. El análisis de riesgo identifica los activos específicos, tales como los componentes del sistema y los datos, por ejemplo, archivos de registro o credenciales que el requisito pretende proteger, así como las amenazas o los resultados de los cuales el requisito protege, por ejemplo, malware, un intruso no detectado o el uso indebido de credenciales. Los ejemplos de factores que podrían contribuir a la probabilidad o al impacto incluyen cualquiera que pueda aumentar la vulnerabilidad de un activo a una amenaza, por ejemplo, la exposición a redes que no son de confianza, la complejidad del entorno o la alta rotación de personal, así como la criticidad de los componentes del sistema o el volumen y la confidencialidad de los datos que están siendo protegidos. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado		
Se mantienen actualizados los conocimientos y la evaluación de los riesgos para el CDE.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		La revisión de los resultados de estos análisis de riesgos específicos al menos una vez cada 12 meses, y de los cambios que podrían afectar el riesgo al medio ambiente, permite a la organización garantizar que los resultados de los análisis de riesgos se mantengan actualizados con los cambios organizacionales y las amenazas, tendencias y tecnologías en evolución, y que las frecuencias establecidas aún responden adecuadamente al nivel de riesgo de la entidad. **Buenas Prácticas** Se recomienda, pero no es obligatoria, una evaluación de riesgos en toda la empresa; se trata de una actividad puntual que permite a las entidades identificar amenazas y vulnerabilidades asociadas, para que las entidades determinen y comprendan amenazas más amplias y emergentes que tienen el potencial de impactar negativamente sus negocios. Esta evaluación de riesgos a nivel de toda la empresa, podría establecerse como parte de un programa de gestión de riesgos global que se utilice como punto de partida para la revisión anual de la política general de seguridad de la información de una organización (consulte el Requisito 12.1.1). Los ejemplos de metodologías de evaluación de riesgos para evaluaciones de riesgos en toda la empresa incluyen, entre otros, ISO *27005* y NIST SP *800-30.*

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
12.3.2 Se realiza un análisis de riesgo específico para cada requisito de PCI DSS que la entidad cumple con el enfoque personalizado, que incluye: • Evidencia documentada detallando cada elemento especificado en el Anexo D: Enfoque personalizado (que incluye, como mínimo, una matriz de controles y análisis de riesgos). • Aprobación de evidencia documentada por parte de la alta dirección. • Realización del análisis de riesgo dirigido al menos una vez cada 12 meses.	**12.3.2** Evalúe el análisis de riesgo personalizado documentado para cada requisito de PCI DSS que la entidad cumple, con el enfoque personalizado, para verificar que la documentación para cada requisito existe y está de acuerdo con todos los elementos especificados en este requisito.	Un análisis de riesgo que sigue una metodología repetible y robusta permite a una entidad cumplir con el objetivo del enfoque personalizado. **Definiciones** El enfoque personalizado para cumplir con un requisito de PCI DSS permite a las entidades definir los controles utilizados para cumplir con el Objetivo del Enfoque Personalizado establecido de un requisito dado de manera que no siga estrictamente el requisito definido. Se espera que estos controles al menos cumplan o superen la seguridad proporcionada por el requisito definido y requieren una documentación extensa por parte de la entidad que utiliza el enfoque personalizado. **Información Adicional** Consulte el Anexo D: Enfoque Personalizado para obtener instrucciones sobre cómo documentar la evidencia requerida para el enfoque personalizado. Consulte Anexo E: Plantillas de muestra para respaldar el enfoque personalizado para conocer las plantillas que las entidades pueden utilizar para documentar sus controles personalizados. Tenga en cuenta que, si bien el uso de las plantillas es opcional, la información especificada dentro de cada plantilla debe documentarse y proporcionarse al asesor de cada entidad.
Objetivo del Enfoque Personalizado		
Este requisito es parte del enfoque personalizado y debe cumplirse para aquellos que utilizan el enfoque personalizado.		
Notas de Aplicabilidad		
Este requisito solo se aplica a las entidades que utilizan un enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
12.3.3 Los protocolos y conjuntos de cifrado criptográfico en uso se documentan y revisan al menos una vez cada 12 meses, incluyendo al menos lo siguiente: • Un inventario actualizado de todos los protocolos y conjuntos de cifrado criptográfico en uso, incluyendo su propósito y dónde se utilizan. • Monitoreo activo de las tendencias de la industria con respecto a la viabilidad continua de todos los protocolos y conjuntos de cifrado criptográfico en uso. • Una estrategia documentada para responder a los cambios anticipados en las vulnerabilidades criptográficas.	**12.3.3** Evalúe la documentación de los protocolos y conjuntos criptográficos en uso y entreviste al personal para verificar que la documentación y la revisión estén de acuerdo con todos los elementos especificados en este requisito.	Los protocolos y las fortalezas del cifrado pueden cambiar rápidamente o quedar obsoletos debido a la identificación de vulnerabilidades o fallas de diseño. Para respaldar las necesidades de seguridad de datos actuales y futuros, las entidades deben saber dónde se usa la criptografía y comprender cómo podría responder rápidamente a los cambios que afectan la fortaleza de sus implementaciones criptográficas. **Buenas Prácticas** La agilidad criptográfica es importante para garantizar que existe una alternativa al método de cifrado original o primitiva criptográfica, con planes para actualizar a la alternativa sin cambios significativos en la infraestructura del sistema. Por ejemplo, si la entidad sabe cuándo los Organismos de Estandarización desaprobarán protocolos o algoritmos, puede realizar planes proactivos para actualizar antes de que la desaprobación tenga un impacto en sus operaciones. **Definiciones** La “agilidad criptográfica” se refiere a la capacidad de monitorear y administrar el cifrado y las tecnologías de verificación relacionadas implementadas en una organización. **Información Adicional** Consulte *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths*.
Objetivo del Enfoque Personalizado		
La entidad puede responder rápidamente a cualquier vulnerabilidad en los protocolos o algoritmos criptográficos cuando esas vulnerabilidades afecten la protección de los datos de titulares de tarjetas.		
Notas de Aplicabilidad		
El requisito se aplica a todos los conjuntos y protocolos criptográficos utilizados para cumplir con los requisitos de PCI DSS. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo** Las tecnologías de hardware y software están en constante evolución, y las organizaciones deben estar al tanto de los cambios en las tecnologías que utilizan, así como de las amenazas en evolución a esas tecnologías, a fin de asegurarse de que puedan prepararse y gestionar vulnerabilidades en hardware y software que no serán remediadas por el proveedor o desarrollador. **Buenas Prácticas** Las organizaciones deben revisar las versiones de firmware para asegurarse de que estén actualizadas y sean respaldadas por los proveedores. Las organizaciones también deben conocer los cambios realizados por los proveedores de tecnología en sus productos o procesos a fin de comprender cómo dichos cambios pueden afectar el uso de cada tecnología por parte de la organización. Las revisiones periódicas de las tecnologías que impactan o influyen en los controles PCI DSS pueden ayudar con las estrategias de compra, uso e implementación, y garantizar que los controles que dependen de esas tecnologías sigan siendo efectivos. Estas revisiones incluyen, entre otras, la revisión de tecnologías que ya no son compatibles con el proveedor y/o que ya no satisfacen las necesidades de seguridad de la organización.
12.3.4 Las tecnologías de hardware y software en uso se revisan al menos una vez cada 12 meses, incluyendo al menos lo siguiente: • Análisis de que las tecnologías continúan recibiendo correcciones de seguridad por parte de los proveedores con prontitud. • Análisis de que las tecnologías continúan apoyando (y no imposibilitan) el cumplimiento PCI DSS de la entidad. • Documentación de cualquier anuncio o tendencia de la industria relacionada con una tecnología, como cuando un proveedor ha anunciado planes para el "fin de la vida útil" de una tecnología. • Documentación de un plan, aprobado por la alta gerencia, para remediar tecnologías obsoletas, incluidas aquellas para las que los proveedores han anunciado planes de "fin de vida útil".	**12.3.4** Evalúe la documentación de las tecnologías de software y hardware en uso y entreviste al personal para verificar que las evaluaciones se hagan de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado Las tecnologías de hardware y software de la entidad están actualizadas y respaldadas por el proveedor. Los planes para eliminar o reemplazar todos los componentes del sistema no admitidos se revisan periódicamente.		
Notas de Aplicabilidad *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
12.4 Gestión del cumplimiento con PCI DSS.		
Requisitos del Enfoque Definido **12.4.1** ***Requisito adicional solo para proveedores de servicios:*** La responsabilidad es establecida por la gerencia ejecutiva para la protección de datos de titulares de tarjetas y un programa de cumplimiento con PCI DSS que incluye: • Responsabilidad general para mantener el cumplimiento PCI DSS. • Definición de un estatuto para un programa de cumplimiento PCI DSS y reporte a la dirección ejecutiva. **Objetivo del Enfoque Personalizado** Los ejecutivos son responsables de la seguridad de los datos de titulares de tarjetas. **Notas de Aplicabilidad** Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios. La dirección ejecutiva puede incluir puestos de nivel C, junta directiva o equivalente. Los títulos específicos dependerán de la estructura organizacional particular. La responsabilidad del programa de cumplimiento PCI DSS se puede asignar a roles individuales y/o a unidades de negocios dentro de la organización.	**Procedimientos de Prueba del Enfoque Definido** **12.4.1** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe la documentación para verificar que la gerencia ejecutiva haya establecido la responsabilidad de la protección de los datos de titulares de tarjeta y un programa de cumplimiento PCI DSS de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** La asignación que hace la gerencia ejecutiva de las responsabilidades de cumplimiento PCI DSS, garantiza la visibilidad, a nivel ejecutivo, del programa de cumplimiento PCI DSS y brinda la oportunidad de generar las preguntas adecuadas para determinar la eficacia del programa e influir en las prioridades estratégicas.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba del Enfoque Definido**	**Objetivo**
12.4.2 *Requisito adicional solo para proveedores de servicios:* Las revisiones se realizan al menos una vez cada tres meses para confirmar que el personal está realizando sus tareas de acuerdo con todas las políticas de Las revisiones son realizadas por personal distinto al responsable de realizar la tarea en cuestión e incluyen, entre otras, las siguientes tareas: • Revisiones de registros diarios. • Revisiones de configuración para controles de seguridad de la red. • Aplicación de estándares de configuración a nuevos sistemas. • Respuesta a las alertas de seguridad. • Procesos de gestión del cambio.	**12.4.2.a *Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe las políticas y los procedimientos para verificar que los procesos estén definidos para conducir revisiones a fin de confirmar que el personal está desarrollando sus tareas de acuerdo con todas las políticas de seguridad y todos los procedimientos operativos, incluyendo, entre otros, las tareas especificadas en este requisito.	La confirmación periódica de que se están siguiendo las políticas y los procedimientos de seguridad garantiza que los controles esperados estén activos y funcionando según lo previsto. Este requisito es distinto de otros requisitos que especifican una tarea a realizar. El objetivo de estas revisiones no es volver a desempeñar con otros requisitos de PCI DSS, sino confirmar que las actividades de seguridad se realizan de manera continua.
Objetivo del Enfoque Personalizado	**12.4.2.b *Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Entreviste al personal responsable y Evalúe los registros de las revisiones para verificar que se realicen de la siguiente manera: • Al menos una vez cada tres meses. • Por personal distinto al responsable de realizar la tarea encomendada.	**Buenas Prácticas**
La efectividad operativa de los controles críticos PCI DSS se verifica periódicamente mediante la inspección manual de los registros.		Estas revisiones también se pueden usar para verificar que se mantenga la evidencia adecuada, por ejemplo, registros de auditoría, informes de exploración de vulnerabilidades, revisiones de conjuntos de reglas de control de seguridad de la red, para ayudar en la preparación de la entidad para su próxima evaluación PCI DSS.
Notas de Aplicabilidad		**Ejemplos**
Este requisito se aplica solo cuando la entidad evaluada es un proveedor de servicios.		Tomando como ejemplo el Requisito 1.2.7, el Requisito 12.4.2 se cumple al confirmar, al menos una vez cada tres meses, que las revisiones de las configuraciones de los controles de seguridad de la red se han realizado con la frecuencia requerida. Por otro lado, el Requisito 1.2.7 se cumple al revisar esas configuraciones como se especifica en el requisito.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
12.4.2.1 ***Requisito adicional solo para proveedores de servicios:*** Las revisiones realizadas de acuerdo con el Requisito 12.4.2 se documentan para incluir: • Resultados de las revisiones. • Acciones de remediación documentadas tomadas para cualquier tarea que no se haya realizado en el Requisito 12.4.2. • Revisión y aprobación de los resultados por parte del personal al que se le haya asignado la responsabilidad del programa de cumplimiento PCI DSS.	**12.4.2.1** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe la documentación de las revisiones realizadas de acuerdo con el requisito 12.4.2 PCI DSS para verificar que la documentación incluya todos los elementos especificados en este requisito.	La intención de estos controles independientes es confirmar si las actividades de seguridad se están realizando de forma continua. Estas revisiones también se pueden usar para verificar que se mantenga la evidencia adecuada, por ejemplo, registros de auditoría, informes de exploración de vulnerabilidades, revisiones de conjuntos de reglas de control de seguridad de la red, para ayudar en la preparación de la entidad para su próxima evaluación PCI DSS.
Objetivo del Enfoque Personalizado		
Los hallazgos de las revisiones de efectividad operacional son evaluados por la gerencia; se implementan las actividades de remediación apropiadas.		
Notas de Aplicabilidad		
Este requisito se aplica solo cuando la entidad evaluada es un proveedor de servicios.		

Requisitos y Procedimientos de Prueba		Guía
12.5 Documentación y validación del alcance PCI DSS.		
Requisitos del Enfoque Definido **12.5.1** Se mantiene y actualiza un inventario de los componentes del sistema que están dentro del alcance PCI DSS, incluyendo una descripción de su función/uso. **Objetivo del Enfoque Personalizado** Todos los componentes del sistema en el ámbito PCI DSS están identificados y son conocidos.	**Procedimientos de Prueba de Enfoque Definido** **12.5.1.a** Evalúe el inventario para verificar que incluya todos los componentes del sistema que son parte del alcance y una descripción de la función/uso de cada uno. **12.5.1.b** Entreviste al personal para verificar que el inventario se mantenga actualizado.	**Objetivo** Mantener una lista actualizada de todos los componentes del sistema permitirá a la organización definir el alcance de su entorno e implementar los requisitos de PCI DSS de manera precisa y eficiente. Sin un inventario, algunos componentes del sistema podrían pasarse por alto y quedar excluidos inadvertidamente de los estándares de configuración de la organización. **Buenas Prácticas** Si una entidad mantiene un inventario de todos los activos, los componentes del sistema dentro del alcance PCI DSS deben ser claramente identificables entre los demás activos. Los inventarios deben incluir depósitos o imágenes que puedan ser instanciadas. Asignar un propietario al inventario ayuda a garantizar que el inventario se mantenga actualizado. **Ejemplos** Algunos métodos para mantener un inventario incluyen una base de datos, una serie de archivos o una herramienta de gestión de inventario.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	
12.5.2 El alcance PCI DSS es documentado y confirmado por la entidad al menos una vez cada 12 meses y ante cambios significativos en el entorno dentro del alcance. Como mínimo, la validación del alcance incluye: • Identificar todos los flujos de datos para las diversas etapas de pago (por ejemplo, autorización, captura de la liquidación, devoluciones y reembolsos) y canales de aceptación (por ejemplo, tarjeta física, tarjeta virtual y comercio electrónico). • Actualizar todos los diagramas de flujo de datos según el Requisito 1.2.4. • Identificar todas las ubicaciones donde se almacenan, procesan y transmiten datos de cuenta, incluidos, entre otros: 1) cualquier ubicación fuera del CDE definida actualmente, 2) aplicaciones que procesan CHD, 3) transmisiones entre sistemas y redes, y 4) copias de seguridad de archivos. • Identificar todos los componentes del sistema en el CDE, conectados al CDE o que podrían afectar la seguridad del CDE. • Identificar todos los controles de segmentación en uso y los entornos desde los que se segmenta el CDE, incluida la justificación de los entornos que están fuera del alcance. • Identificar todas las conexiones de entidades de terceros con acceso al CDE. • Confirmar que todos los flujos de datos identificados, datos de cuentas, componentes del sistema, controles de segmentación y conexiones de terceros con acceso al CDE están incluidos en el alcance.	**12.5.2.a** Evalúe los resultados documentados de las revisiones del alcance y entreviste al personal para verificar que se realicen las revisiones: • Al menos una vez cada 12 meses. • Después de cambios significativos en el entorno dentro del alcance. **12.5.2.b** Evalúe los resultados documentados de las revisiones del alcance realizadas por la entidad para verificar que la actividad de confirmación del alcance PCI DSS incluye todos los elementos especificados en este requisito.	**Objetivo** La validación frecuente del alcance PCI DSS ayuda a garantizar que el alcance PCI DSS permanezca actualizado y alineado con los objetivos de negocios cambiantes y, por lo tanto, que los controles de seguridad protejan todos los componentes apropiados del sistema. **Buenas Prácticas** El alcance preciso implica evaluar críticamente el CDE y todos los componentes del sistema conectado para determinar la cobertura necesaria para los requisitos de PCI DSS. Las actividades de alcance, incluido el análisis detallado y el monitoreo continuo, ayudan a garantizar que los sistemas dentro del alcance estén debidamente protegidos. Al documentar las ubicaciones de los datos de la cuenta, la entidad puede considerar crear una tabla u hoja de cálculo que incluya la siguiente información: • Almacenamiento de datos (bases de datos, archivos, nube, etc.), incluyendo el propósito del almacenamiento de datos y el período de retención, • Qué elementos de CHD se almacenan (datos PAN, fecha de caducidad, nombre del titular de la tarjeta y/o cualquier elemento de SAD antes de completar la autorización), • Cómo se protegen los datos (tipo de cifrado y robustez, algoritmo *hash* y solidez, truncamiento, *tokenización),* • Cómo se registra el acceso a las bodegas de datos, incluyendo una descripción de los mecanismos de registro en uso (solución empresarial, nivel de aplicación, nivel de sistema operativo, etc.). *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado El alcance PCI DSS se verifica periódicamente, y después de cambios significativos, mediante un análisis integral y las medidas técnicas apropiadas. **Notas de Aplicabilidad** Se espera que esta confirmación anual del alcance PCI DSS sea una actividad realizada por la entidad que se está evaluando, y no es la misma, ni pretende ser reemplazada por, la confirmación del alcance realizada por el asesor de la entidad durante la evaluación anual.		Además de los sistemas y redes internos, todas las conexiones de entidades de terceros, por ejemplo, socios de negocios, entidades que brindan servicios de apoyo remoto y otros proveedores de servicios, deben identificarse para determinar la inclusión en el alcance PCI DSS. Una vez que se han identificado las conexiones dentro del alcance, se pueden implementar los controles PCI DSS aplicables para reducir el riesgo de que se utilice una conexión de terceros para comprometer al CDE de una entidad. Se puede usar una herramienta o metodología de descubrimiento de datos para facilitar la identificación de todas las fuentes y ubicaciones de datos PAN, y para buscar datos PAN que residen en sistemas y redes fuera del CDE definido actualmente o en lugares inesperados dentro del CDE definido, por ejemplo, en un registro errado o en un archivo de volcado de memoria. Este enfoque puede ayudar a garantizar que se detecten ubicaciones previamente desconocidas de datos PAN y que los datos PAN se eliminen o se aseguren adecuadamente. **Información Adicional** Para obtener orientación adicional, refiérase a la *Información Complementaria: Guía para el Alcance y la Segmentación de la Red PCI DSS*.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
12.5.2.1 ***Requisito adicional solo para proveedores de servicios:*** El alcance PCI DSS es documentado y confirmado por la entidad al menos una vez cada seis meses y ante cambios significativos en el entorno dentro del alcance. Como mínimo, la validación del alcance incluye todos los elementos especificados en el Requisito 12.5.2.	**12.5.2.1.a** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe los resultados documentados de las revisiones del alcance y entreviste al personal para verificar que se realicen las revisiones relacionadas con el Requisito 12.5.2: • Al menos una vez cada seis meses, y • Después de cambios significativos.	Típicamente los proveedores de servicios tienen acceso a mayores volúmenes de datos de titulares de tarjetas que los comerciantes, o pueden o proporcionar un punto de entrada que se puede explotar para luego comprometer a muchas otras entidades. Los proveedores de servicios también suelen tener redes más amplias y complejas que están sujetas a cambios más frecuentes. La probabilidad de que se pasen por alto los cambios en el alcance de las redes complejas y dinámicas es mayor en los entornos de los proveedores de servicios. Es probable que la validación del alcance PCI DSS con más frecuencia descubra dichos cambios pasados por alto antes de que un atacante pueda explotarlos.
Objetivo del Enfoque Personalizado	**12.5.2.1.b** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe los resultados documentados de las revisiones del alcance para verificar que la validación del alcance incluya todos los elementos especificados en el Requisito 12.5.2.	
La precisión del alcance PCI DSS se verifica para que sea continuamente precisa mediante un análisis integral y las medidas técnicas apropiadas.		
Notas de Aplicabilidad		
Este requisito sólo aplica cuando la entidad que se evalúa es un proveedor de servicios. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo** La estructura y la gestión de una organización definen los requisitos y el protocolo para operaciones eficientes y seguras. Los cambios en esta estructura podrían tener efectos negativos en los controles y marcos existentes al reasignar o eliminar recursos que alguna vez respaldaron los controles PCI DSS o al heredar nuevas responsabilidades que pueden no tener controles establecidos. Por lo tanto, es importante revisar el alcance y los controles PCI DSS cuando haya cambios en la estructura y administración de una organización para garantizar que los controles estén implementados y activos. **Ejemplos** Los cambios en la estructura organizativa incluyen, entre otros, fusiones o adquisiciones de empresas y cambios significativos o reasignaciones de personal responsable de los controles de seguridad.
12.5.3 ***Requisito adicional solo para proveedores de servicios:*** Los cambios significativos en la estructura organizativa dan como resultado una revisión documentada (interna) del impacto en el alcance PCI DSS y la aplicabilidad de los controles; los resultados se comunican a la dirección ejecutiva.	**12.5.3.a** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe las políticas y los procedimientos para verificar que los procesos estén definidos de tal manera que un cambio significativo en la estructura organizacional resulte en una revisión documentada del impacto en el alcance y la aplicabilidad de los controles PCI DSS.	
Objetivo del Enfoque Personalizado El alcance PCI DSS se confirma después de un cambio organizacional significativo.	**12.5.3.b** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe la documentación (por ejemplo, las actas de las reuniones) y entreviste al personal responsable a fin de verificar que los cambios significativos en la estructura organizacional dieron como resultado revisiones documentadas que incluyeron todos los elementos especificados en este requisito, y los resultados se comunicaron a la dirección ejecutiva.	
Notas de Aplicabilidad Este requisito se aplica solo cuando la entidad evaluada es un proveedor de servicios. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
12.6 La educación en concientización sobre la seguridad es una actividad continua.		
Requisitos del Enfoque Definido **12.6.1** Se implementa un programa formal de concientización sobre seguridad para que todo el personal conozca la política y los procedimientos de seguridad de la información a de la entidad, y el rol del personal en la protección de los datos de titulares de tarjetas. **Objetivo del Enfoque Personalizado** El personal conoce el panorama de las amenazas, su responsabilidad en el funcionamiento de los controles de seguridad pertinentes y puede tener acceso a la asistencia y orientación cuando lo necesite.	**Procedimientos de Prueba de Enfoque Definido** **12.6.1** Evalúe el programa de concientización sobre seguridad para verificar que brinda conocimiento a toda la personal acera de las políticas y procedimientos de seguridad de la información de la entidad, y el rol del personal en la protección de los datos de titulares de tarjetas.	**Objetivo** Si el personal no está informado sobre las políticas y los procedimientos de seguridad de la información de su empresa y de sus propias responsabilidades en materia de seguridad, las garantías y los procesos de seguridad que se han implementado pueden volverse ineficientes debido a errores no intencionales o acciones intencionales.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **12.6.2** El programa de concientización sobre seguridad es: • Revisado al menos una vez cada 12 meses, y • Actualizado según sea necesario para abordar cualquier nueva amenaza y vulnerabilidad que pueda impactar la seguridad del CDE de la entidad, o la información proporcionada al personal sobre sus funciones en lo concerniente a la protección de los datos de titulares de tarjetas. **Objetivo del Enfoque Personalizado** El contenido del material de concientización sobre seguridad se revisa y actualiza periódicamente. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba de Enfoque Definido** **12.6.2** Evalúe el contenido del programa de concientización sobre seguridad, la evidencia de las revisiones y entreviste al personal para verificar que el programa de concientización sobre seguridad cumpla con todos los elementos especificados en este requisito.	**Objetivo** El entorno de amenazas y las defensas de una entidad no son estáticos. Como tal, los materiales del programa de concientización sobre seguridad deben actualizarse con la frecuencia necesaria para garantizar que la educación recibida por el personal esté actualizada y represente el entorno de amenazas actual.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	
12.6.3 El personal recibe capacitación sobre seguridad de la siguiente manera: • Al momento de la contratación y al menos una vez cada 12 meses. • A través de múltiples métodos de comunicación. • El personal reconoce al menos una vez cada 12 meses que ha leído y comprendido las políticas y los procedimientos de seguridad de la información.	**12.6.3.a** Evalúe los registros del programa de concientización sobre seguridad para verificar que el personal asista a la capacitación de concientización sobre seguridad al momento de la contratación y al menos una vez cada 12 meses. **12.6.3.b** Evalúe los materiales del programa de concientización sobre seguridad para verificar que este incluya múltiples métodos para comunicar la concientización y educar al personal. **12.6.3.c** Entreviste al personal para verificar que hayan completado la capacitación de concientización y que sean conscientes de su función en la protección de los datos de titulares de tarjetas. **12.6.3.d** Evalúe los materiales del programa de concientización sobre seguridad y los reconocimientos del personal para verificar que reconocen, al menos una vez cada 12 meses, que han leído y entendido la política y los procedimientos de seguridad de la información.	**Objetivo** La capacitación del personal garantiza que reciban la información sobre la importancia de la seguridad de la información y que comprendan el papel que juega en la protección de la organización. Solicitar el reconocimiento por parte del personal ayuda a garantizar que hayan leído y comprendido las políticas y los procedimientos de seguridad, y que se hayan comprometido y seguirán comprometiéndose a cumplir con estas políticas. **Buenas Prácticas** Las entidades pueden incorporar capacitación para nuevos empleados como parte del proceso de incorporación de Recursos Humanos. La capacitación debe describir los "hacer" y "no hacer" relacionados con la seguridad. La capacitación periódica de actualización refuerza los procesos y procedimientos de seguridad esenciales que pueden olvidarse o pasarse por alto. Las entidades deberían considerar brindar capacitación sobre concientización en materia de seguridad cada vez que el personal se transfiera a otras funciones en las que se pueda afectar la seguridad de los datos de cuentas desde funciones en las que no tuvo este impacto. Los métodos y el contenido de la capacitación pueden variar, según las funciones del personal. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado El personal permanece actualizado y en conocimiento sobre las amenazas, sobre su responsabilidad en el funcionamiento de los controles de seguridad pertinentes y puede obtener asistencia y orientación cuando sea necesarias.		**Ejemplos** Los diferentes métodos que se pueden utilizar para concientizar y educar sobre seguridad incluyen carteles, cartas, capacitación virtual, capacitación presencial, reuniones de equipo e incentivos. Los reconocimientos del personal pueden registrarse por escrito o electrónicamente.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
12.6.3.1 El entrenamiento de concientización de seguridad incluye la concientización ante amenazas y vulnerabilidades que podrían impactar la seguridad del CDE, incluyendo, pero no limitado a: • *Phishing* y ataques relacionados. • Ingeniería social.	**12.6.3.1** Evalúe el contenido de la capacitación de concientización en materia de seguridad, para verificar que incluye todos los elementos especificados en este requisito.	A fin de minimizar la probabilidad de un ataque exitoso, es esencial educar al personal sobre cómo detectar, reaccionar y reportar potenciales ataques de *phishing* y otros, así como intentos de ingeniería social. **Buenas Prácticas** Un programa eficiente de concientización sobre la seguridad debe incluir ejemplos de correos electrónicos de *phishing* y pruebas periódicas para determinar la prevalencia del personal que informa de dichos ataques. El material de capacitación que una entidad puede considerar para este tema incluye: • Cómo identificar el *phishing* y otros ataques de ingeniería social. • Cómo reaccionar ante una sospecha de *phishing* y de ingeniería social. • Dónde y cómo denunciar las actividades sospechosas de phishing e ingeniería social. El énfasis en la denuncia permite a la organización recompensar el comportamiento positivo, optimizar las defensas técnicas (véase el Requisito 5.4.1) y tomar medidas inmediatas para eliminar correos electrónicos de *phishing* similares que evadieron las defensas técnicas de las bandejas de entrada de los destinatarios.
Objetivo del Enfoque Personalizado		
El personal es consciente de sus propias vulnerabilidades humanas y de cómo los actores de amenazas intentarán explotar dichas vulnerabilidades. El personal puede recibir asistencia y orientación cuando sea necesario.		
Notas de Aplicabilidad		
Véase el requisito 5.4.1 para obtener orientación sobre la diferencia entre los controles técnicos y automatizados para detectar y proteger a los usuarios de los ataques de *phishing* y este requisito, para proporcionar a los usuarios capacitación en concientización sobre seguridad en materia de suplantación de identidad e ingeniería social. Se trata de dos requisitos distintos y separados, y uno de ellos no se cumple aplicando los controles exigidos por el otro. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **12.6.3.2** La capacitación en concientización sobre seguridad incluye la concientización sobre el uso aceptable de las tecnologías de usuario final de acuerdo con el requisito 12.2.1. **Objetivo del Enfoque Personalizado** El personal es consciente de su responsabilidad en materia de seguridad y operación de las tecnologías de usuario final, y es capaz de obtener asistencia y orientación cuando sea necesario. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba de Enfoque Definido** **12.6.3.2** Evalúe el contenido en materia de capacitación sobre concientización de la seguridad para verificar que incluya la concientización sobre el uso aceptable de las tecnologías del usuario final de acuerdo con el Requisito 12.2.1.	**Objetivo** Al incluir los puntos clave de la política de uso aceptable en la capacitación regular y en el contexto relacionado, el personal entenderá sus responsabilidades y cómo éstas impactan la seguridad de los sistemas de la organización.

Requisitos y Procedimientos de Prueba		Guía
12.7 El personal es evaluado para reducir los riesgos de amenazas internas.		
Requisitos del Enfoque Definido **12.7.1** El personal potencial que tendrá acceso al CDE es investigado, en el marco de las limitaciones que establecen las leyes locales, antes de su contratación, a fin de minimizar el riesgo de ataques provenientes de fuentes internas. **Objetivo del Enfoque Personalizado** Se comprende y gestiona el riesgo relacionado con el hecho de permitir a los nuevos miembros del personal el acceso al CDE. **Notas de Aplicabilidad** Para el personal potencial que vaya a ser contratado para puestos como los de cajeros en tiendas, que sólo tienen acceso a un número de tarjeta a la vez cuando facilitan una transacción, este requisito es sólo una recomendación.	**Procedimientos de Prueba de Enfoque Definido** **12.7.1** Entreviste a la gerencia responsable del Departamento de Recursos Humanos para verificar que se realice una evaluación, el marco de las limitaciones que establecen las leyes locales, antes de contratar al personal potencial que tendrá acceso al CDE.	**Objetivo** La realización de una selección exhaustiva antes de contratar al personal potencial que tendría acceso al CDE, proporciona a las entidades la información necesaria para tomar decisiones de riesgo informadas con respecto al personal que contratan y que tendrá acceso al CDE. Otros beneficios de la evaluación de personal potencial incluyen ayudar a garantizar la seguridad en el lugar de trabajo y confirmar la información proporcionada por los posibles empleados en sus currículos. **Buenas Prácticas** Las entidades deben considerar la posibilidad de evaluar al personal existente cada vez que sean transferidos de funcione sin acceso al CDE a otras funciones en las que tengan acceso al CDE, Para que sea eficiente, el nivel de evaluación debe ser adecuado para el puesto. Por ejemplo, los puestos que requieren una mayor responsabilidad o que tienen acceso administrativo a datos o sistemas críticos pueden justificar un control más detallado o más frecuente que los puestos con menos responsabilidad y acceso. **Ejemplos** Las opciones de selección pueden incluir, según sea apropiado para la región de la entidad, el historial de empleo anterior, la revisión de información pública/recursos de medios sociales, los antecedentes penales, el historial de crédito y la comprobación de referencias.

Requisitos y Procedimientos de Prueba		Guía
12.8 Gestión del riesgo de los activos de información asociados a las relaciones con proveedores de servicios externos (TPSP).		
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo** Mantener una lista de todos los TPSP identifica dónde se extiende el riesgo potencial fuera de la organización y define la superficie de ataque extendida de la organización. **Ejemplos** Los diferentes tipos de TPSP incluyen aquellos que: • Almacenan, procesan o transmiten datos de cuentas en nombre de la entidad (como pasarelas de pago, procesadores de pago, proveedores de servicios de pago (PSP) y proveedores de almacenamiento externo). • Gestionan los componentes del sistema incluidos en la evaluación PCI DSS de la entidad (como los proveedores de servicios de control de protección de la red, los servicios antimalware y la gestión de incidentes y eventos de seguridad (SIEM); los centros de contacto y de llamadas; las empresas de alojamiento web; y los proveedores de nube IaaS, PaaS, SaaS y FaaS). • Podría afectar la seguridad del CDE de la entidad (como los proveedores que prestan asistencia mediante acceso remoto y los desarrolladores de software a medida).
12.8.1 Se mantiene una lista de todos los proveedores de servicios de terceros (TPSP) con los que se comparten datos de cuentas o que podrían afectar a la seguridad de los datos de cuentas, incluyendo una descripción para cada uno de los servicios prestados.	**12.8.1.a** Evalúe las políticas y procedimientos para comprobar que se han definido procesos para mantener una lista de TPSPS incluyendo una descripción de cada uno de los servicios suministrados, para todos los TPSP con los que se comparten datos de cuentas o que podrían afectar la seguridad de los datos del tarjetahabiente.	
	12.8.1.b Evalúe la documentación para verificar que se mantiene una lista de todos los TPSP que incluya una descripción de los servicios prestados.	
Objetivo del Enfoque Personalizado		
Se mantienen registros de los TPSP y de los servicios prestados.		
Notas de Aplicabilidad		
El uso de un TPSP que cumpla con PCI DSS no hace que una entidad esté en cumplimiento con PCI DSS, ni elimina la responsabilidad de la entidad por su propio cumplimiento PCI DSS.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
12.8.2 Se mantienen acuerdos escritos con los TPSP de la siguiente manera: • Se mantienen acuerdos escritos con todos los TPSP con los que se comparten datos de cuentas o que podrían afectar la seguridad del CDE. • Los acuerdos escritos incluyen el reconocimiento por parte de los TPSP de que son responsables por la seguridad de los datos de cuentas que los TPSP poseen o almacenan, procesan o transmiten en nombre de la entidad, o en la medida en que puedan afectar a la seguridad del CDE de la entidad.	**12.8.2.a** Evalúe las políticas y los procedimientos para verificar que los procesos están definidos para mantener los acuerdos escritos con todos los TPSP de acuerdo con todos los elementos especificados en este requisito.	El reconocimiento por escrito de un TPSP demuestra su compromiso de mantener la seguridad adecuada para los datos de cuentas que se obtienen de los clientes y que el TPSP es plenamente consciente de los activos que podrían verse afectados durante el suministro del servicio del TPSP. La medida en que un TPSP específico es responsable de la seguridad de los datos de cuentas, dependerá del servicio prestado y del acuerdo entre el proveedor y la entidad evaluada (el cliente). Junto con el Requisito 12.9.1, este requisito tiene por objeto promover un nivel de comprensión coherente entre las partes, en relación con sus responsabilidades aplicables en el marco PCI DSS. Por ejemplo, el acuerdo puede incluir los requisitos de PCI DSS aplicables que deben mantenerse como parte del servicio prestado.
Objetivo del Enfoque Personalizado	**12.8.2.b** Evalúe los acuerdos escritos con los TPSP para verificar que se mantienen de acuerdo con todos los elementos especificados en este requisito.	**Buenas Prácticas**
Se mantienen registros del reconocimiento por parte de cada TPSP, de su responsabilidad en proteger los datos de cuentas.		La entidad también puede considerar la posibilidad de incluir en su acuerdo escrito con un TPSP que éste apoyará la solicitud de información de la entidad según el Requisito 12.9.2. Las entidades también querrán saber si algún TPSP tiene relaciones "anidadas" con otros TPSP, lo que significa que el TPSP principal contrata a otro(s) TPSP para la prestación de un servicio. Es importante comprender si el TPSP principal depende de los TPSP secundarios para lograr el cumplimiento general de un servicio, y qué tipos de acuerdos escritos tiene el TPSP principal con los TPSP secundarios. Las entidades pueden considerar la posibilidad de incluir en su acuerdo escrito la cobertura de cualquier TPSP "anidado" que un TPSP primario pueda utilizar. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad La redacción exacta de un reconocimiento dependerá del acuerdo entre las dos partes, los detalles del servicio que se presta y las responsabilidades asignadas a cada parte. El reconocimiento no tiene que incluir la redacción exacta prevista en este requisito. La prueba de que un TPSP cumple con los requisitos de PCI DSS (por ejemplo, un certificado de cumplimiento PCI DSS (AOC) o una declaración en el sitio web de la empresa) no es lo mismo que el acuerdo escrito especificado en este requisito.		**Información Adicional** Refiérase a la *Información Complementaria:* Para mayor información refiérase a *Garantía de Seguridad de Terceros.*
Requisitos del Enfoque Definido **12.8.3** Se implementa un proceso establecido para contratar a los TPSP, incluyendo la debida diligencia antes de la contratación. **Objetivo del Enfoque Personalizado** La capacidad, la intención y los recursos de un posible TPSP para proteger adecuadamente los datos del tarjetahabiente se evalúan antes de contratar al TPSP.	**Procedimientos de Prueba de Enfoque Definido** **12.8.3.a** Evalúe las políticas y los procedimientos para verificar que se han definido los procesos para la contratación de TPSP, incluyendo la debida diligencia antes de la contratación. **12.8.3.b** Evalúe las evidencias y entreviste al personal responsable para verificar que el proceso de contratación de TPSP incluye la debida diligencia antes de la contratación.	**Objetivo** Un proceso minucioso para la contratación de TPSP, que incluya detalles para la selección y el examen antes de la contratación, ayuda a garantizar que un TPSP sea examinado a fondo internamente por una entidad antes de establecer una relación formal y que se comprenda el riesgo para los datos de titulares de tarjetas asociado a la contratación de un TPSP. **Buenas Prácticas** Los procesos y objetivos específicos de diligencia debida variarán en cada organización. Entre los elementos que deben tenerse en cuenta están las prácticas de notificación del proveedor, los procedimientos de notificación de infracciones y de respuesta a incidentes, los detalles de cómo se asignan las responsabilidades relacionadas con PCI DSS entre cada una de las partes, cómo el TPSP valida el cumplimiento con PCI DSS y qué pruebas aporta.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
12.8.4 Se implementa un programa para monitorear el estado de cumplimiento PCI DSS de los TPSP al menos una vez cada 12 meses.	**12.8.4.a** Evalúe las políticas y los procedimientos para verificar que los procesos para monitorear el estado de cumplimiento PCI DSS de los TPSP al menos una vez cada 12 meses, estén definidos.	Conocer el estado de cumplimiento PCI DSS de todos los TPSP contratados proporciona seguridad y conocimiento sobre si se está cumpliendo con los requisitos aplicables a los servicios que ofrecen a la organización.
	12.8.4.b Evalúe la documentación y entreviste al personal responsable de verificar que el estado de cumplimiento PCI DSS de cada TPSP sea supervisado al menos una vez cada 12 meses.	**Buenas Prácticas** Si el TPSP ofrece una variedad de servicios, el estado de cumplimiento que la entidad supervisa debe ser específico para los servicios prestados a la entidad y para los servicios en el ámbito de la evaluación PCI DSS de la entidad. Si un TPSP tiene un certificado de cumplimiento PCI DSS (AOC), se espera que el TPSP lo proporcione a los clientes que lo soliciten para demostrar su estado de cumplimiento con PCI DSS. Si el TPSP no se ha sometido a una evaluación PCI DSS, este puede proporcionar otras evidencias para demostrar que se ha cumplido con los requisitos aplicables sin someterse a una validación formal del cumplimiento. Por ejemplo, el TPSP puede proporcionar evidencias específicas al asesor de la entidad para que éste pueda confirmar que se cumple con los requisitos aplicables. Alternativamente, el TPSP puede optar por someterse a varias evaluaciones a solicitud de cada uno de los asesores de sus clientes; cada evaluación estaría dirigida a confirmar que se cumplen los requisitos aplicables. **Información Adicional** Para obtener más información sobre los proveedores de servicios externos, consulte: • Sección PCI DSS: Uso de Proveedores de Servicios Externos. • *Información complementaria: Garantía de Seguridad de Terceros*.
Objetivo del Enfoque Personalizado		
El estado de cumplimiento PCI DSS de los TPSP se verifica periódicamente.		
Notas de Aplicabilidad		
Cuando una entidad tiene un acuerdo con un TPSP para cumplir con los requisitos de PCI DSS en nombre de la entidad (por ejemplo, a través de un servicio de *firewall*), la entidad debe trabajar con el TPSP para asegurarse de que se cumplan los requisitos de PCI DSS aplicables. Si el TPSP no cumple con los requisitos de PCI DSS aplicables, entonces, esos requisitos también están “no en cumplimiento” para la entidad.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo** Es importante que la entidad comprenda qué requisitos y sub-requisitos de PCI DSS han acordado cumplir sus TPSP, qué requisitos se comparten entre el TPSP y la entidad, y para aquellos que se comparten, brindar detalles sobre cómo se comparten los requisitos y qué entidad es responsable de cumplir con cada sub-requisito. Sin este entendimiento compartido, es inevitable que la entidad y el TPSP asuman que un sub-requisito de PCI DSS es responsabilidad de la otra parte, y por lo tanto, es posible que ese sub-requisito no se aborde en absoluto. La información específica que una entidad mantenga dependerá del acuerdo particular con sus proveedores, el tipo de servicio, etc. Los TPSP pueden definir sus responsabilidades en cuanto a PCI DSS de manera que sean las mismas para todos sus clientes; en caso contrario, estas responsabilidades deberán ser acordadas tanto por la entidad como por el TPSP. **Buenas Prácticas** Las entidades pueden documentar estas responsabilidades a través de una matriz que identifica todos los requisitos de PCI DSS aplicables e indica para cada requisito si la entidad o el TPSP es responsable de cumplir con ese requisito o si es una responsabilidad compartida. Este tipo de documento a menudo se denomina *matriz de responsabilidad.* *(continúa en la página siguiente)*
12.8.5 Se mantiene información sobre qué requisitos de PCI DSS gestiona cada TPSP, cuáles gestiona la entidad y cualquiera que se comparta entre el TPSP y la entidad.	**12.8.5.a** Evalúe las políticas y los procedimientos para verificar que los procesos estén definidos para mantener información sobre qué requisitos de PCI DSS administra cada TPSP, cuáles administra la entidad y cualquiera que se comparta entre ambos, el TPSP y la entidad.	
Objetivo del Enfoque Personalizado	**12.8.5.b** Evalúe la documentación y entreviste al personal para verificar que la entidad mantenga información sobre qué requisitos de PCI DSS administra cada TPSP, cuáles administra la entidad y cualquiera que sea compartido entre ambas entidades.	
Los registros que detallan los requisitos de PCI DSS y los componentes del sistema relacionados, por los cuales cada TPSP es único o conjuntamente responsable, se mantienen y revisan periódicamente.		

Requisitos y Procedimientos de Prueba		Guía
		También es importante que las entidades entiendan si algún TPSP tiene relaciones "anidadas" con otros TPSP, lo que significa que el TPSP primario contrata con otro(s) TPSP(s) con el fin de proporcionar un servicio. Es importante comprender si el TPSP principal se basa en los TPSP secundarios para lograr el cumplimiento general de un servicio y cómo el TPSP principal supervisa el rendimiento del servicio y el estado de cumplimiento PCI DSS de los TPSP secundarios. Tenga presente que es responsabilidad del TPSP primario administrar y monitorear cualquier TPSP secundario. **Información Adicional** Refiérase a la *Información Complementaria: Garantía de Seguridad de Terceros* para una muestra de modelo de matriz de responsabilidad.

Requisitos y Procedimientos de Prueba		Guía
12.9 Los proveedores de servicios externos (TPSP) respaldan el cumplimiento PCI DSS de sus clientes.		
Requisitos del Enfoque Definido **12.9.1** ***Requisito adicional solo para proveedores de servicios:*** Los TPSP reconocen por escrito a los clientes que son responsables por la seguridad de los datos de cuentas que el TPSP posee o almacena, procesa o transmite en nombre del cliente, o en la medida en que puedan afectar la seguridad del CDE del cliente. **Objetivo del Enfoque Personalizado** Los TPSP reconocen formalmente sus responsabilidades de seguridad hacia sus clientes. **Notas de Aplicabilidad** Este requisito se aplica solo cuando la entidad evaluada es un proveedor de servicios. La redacción exacta de un reconocimiento dependerá del acuerdo entre las dos partes, los detalles del servicio que se presta y las responsabilidades asignadas a cada parte. El reconocimiento no tiene que incluir la redacción exacta prevista en este requisito.	**Procedimientos de Prueba de Enfoque Definido** **12.9.1** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe las políticas, los procedimientos y las plantillas de TPSP que se utilizan para los acuerdos escritos a fin de verificar que los procesos estén definidos, de manera que el TPSP proporcione un reconocimiento por escrito a los clientes, de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Junto con el Requisito 12.8.2, este requisito tiene por objeto promover un nivel de comprensión coherente entre los TPSP y sus clientes acerca de sus responsabilidades aplicables en el marco PCI DSS. El reconocimiento de los TPSP evidencia su compromiso de mantener la seguridad adecuada de los datos de cuenta que obtiene de sus clientes. El método por el cual los TPSP proporcionan un reconocimiento por escrito debe ser acordado entre el proveedor y sus clientes.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	
12.9.2 ***Requisito adicional solo para proveedores de servicios:*** Los TPSP respaldan las solicitudes de información de sus clientes para cumplir con los Requisitos 12.8.4 y 12.8.5 proporcionando lo siguiente a pedido del cliente: • Información del estado de cumplimiento PCI DSS para cualquier servicio que el TPSP realice en nombre de los clientes (Requisito 12.8.4). • Información sobre qué requisitos de PCI DSS son responsabilidad del TPSP y cuáles son responsabilidad del cliente, incluyendo las responsabilidades compartidas (Requisito 12.8.5).	**12.9.2** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe las políticas y los procedimientos para verificar que los procesos estén definidos para que los TPSP respalden la solicitud de información de los clientes para cumplir con los Requisitos 12.8.4 y 12.8.5 de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Si un TPSP no proporciona la información necesaria para permitir que sus clientes cumplan con sus requisitos de seguridad y cumplimiento, los clientes no podrán proteger los datos de titulares de tarjetas ni podrán cumplir con sus propias obligaciones contractuales. **Buenas Prácticas** Si un TPSP tiene un certificado de cumplimiento PCI DSS (AOC), se espera que el TPSP lo proporcione a los clientes que lo soliciten para demostrar su estado de cumplimiento con PCI DSS. Si el TPSP no se ha sometido a una evaluación PCI DSS, estos pueden proporcionar otras evidencias para demostrar que se ha cumplido con los requisitos aplicables sin someterse a una validación formal del cumplimiento. Por ejemplo, el TPSP puede proporcionar evidencias específicas al asesor de la entidad para que éste pueda confirmar que se cumple con los requisitos aplicables. Alternativamente, el TPSP puede optar por someterse a varias evaluaciones a solicitud de cada uno de los asesores de sus clientes; cada evaluación estaría dirigida a confirmar que se cumplen los requisitos aplicables. Los TPSP deben proporcionar evidencias suficientes a sus clientes para verificar que el alcance de la evaluación PCI DSS del TPSP cubrió los servicios aplicables al cliente, que los requisitos de PCI DSS relevantes fueron evaluados y se determinó que estaban en cumplimiento. *(continúa en la página siguiente)*
Objetivo del Enfoque Personalizado		
Los TPSP brindan información según sea necesario para respaldar los esfuerzos de cumplimiento con PCI DSS por parte de sus clientes.		
Notas de Aplicabilidad		
Este requisito se aplica solo cuando la entidad evaluada es un proveedor de servicios.		

Requisitos y Procedimientos de Prueba		Guía
		Los TPSP pueden definir sus responsabilidades PCI DSS para que sean las mismas para todos sus clientes; de otra forma, esta responsabilidad deberá ser acordada tanto por el cliente como por el TPSP. Es importante que el cliente comprenda qué requisitos y sub-requisitos de PCI DSS han acordado cumplir sus TPSP; qué requisitos se comparten entre el TPSP y el cliente, y para aquellos que se comparten, brindar detalles sobre cómo se comparten los requisitos y qué entidad es responsable de cumplir con cada sub-requisito. Un ejemplo de la forma de documentar estas responsabilidades es a través de una matriz que identifica todos los requisitos de PCI DSS aplicables e indica si el cliente o el TPSP es responsable de cumplir con ese requisito o si es una responsabilidad compartida. **Información Adicional** Para obtener más orientación, consulte: • Sección PCI DSS: Uso de Proveedores de Servicios Externos. • Información complementaria: Garantía de seguridad de terceros (incluye una plantilla de modelo de matriz de responsabilidad).

Requisitos y Procedimientos de Prueba		Guía
12.10 Respuesta inmediata a incidentes de seguridad sospechosos y confirmados que podrían afectar al CDE.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	
12.10.1 Existe un plan de respuesta a incidentes y está listo para activarse en caso de sospecha o confirmación de un incidente de seguridad. El plan incluye, pero no se limita a: • Funciones, responsabilidades y estrategias de comunicación y contacto en caso de sospecha o confirmación de un incidente de seguridad, incluyendo la notificación de marcas de pago y adquirentes, como mínimo. • Procedimientos de respuesta a incidentes con actividades específicas de contención y mitigación para diferentes tipos de incidentes. • Procedimientos de recuperación y continuidad del negocio. • Procesos de apoyo de datos. • Análisis de requisitos legales para reportar situaciones comprometidas. • Cobertura y respuestas de todos los componentes críticos del sistema. • Referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago.	**12.10.1.a** Evalúe el plan de respuesta a incidentes para verificar que exista e incluya al menos los elementos especificados en este requisito. **12.10.1.b** Entreviste al personal y Evalúela documentación de incidentes o alertas reportados previamente para verificar si se siguieron los procedimientos y el plan de respuesta a incidentes documentados.	**Objetivo** Sin un plan integral de respuesta a incidentes, que las partes responsables difundan, lean y entiendan adecuadamente, la confusión y la falta de respuestas conjuntas podrían incrementar el tiempo de inactividad del negocio, exposición innecesaria a los medios públicos, así como riesgos financieros y/o de pérdida de reputación, y responsabilidades legales. **Buenas Prácticas** El plan de respuesta a incidentes debe ser minucioso y contener todos los elementos clave para las partes interesadas (por ejemplo, legales, comunicaciones) permitiendo a la entidad responder de manera eficiente en caso de una filtración que podría afectar los datos de cuentas. Es importante mantener el plan actualizado con la información de contacto actual de todas las personas designadas para desempeñar un papel en la respuesta a incidentes. Otras partes relevantes al momento de enviar notificaciones pueden incluir clientes, instituciones financieras (adquirentes y emisores) y socios de negocios. Las entidades deben considerar cómo abordar todas tipos de compromisos a los datos del CDE, en sus planes de respuesta a incidentes, incluidos los datos de cuentas, claves de cifrado inalámbricas, claves de cifrado utilizadas para la transmisión y el almacenamiento o datos de cuentas o datos de titulares de tarjetas, etc. *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Se mantiene un plan integral de respuesta a incidentes que cumpla con las expectativas de la marca de la tarjeta.		**Ejemplos** Los requisitos legales para reportar compromisos incluyen los de la mayoría de los estados de los Estados Unidos, el Reglamento General de Protección de Datos (GDPR) de la UE y la Ley de Protección de Datos Personales (Singapur). **Información Adicional** Para obtener más información, consulte *NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide*.
Requisitos del Enfoque Definido **12.10.2** Al menos una vez cada 12 meses, el plan de respuesta a incidentes de seguridad es: • Revisado y el contenido actualizado según sea necesario. • Probado, incluyendo todos los elementos enumerados en el Requisito 12.10.1.	**Procedimientos de Prueba de Enfoque Definido** **12.10.2** Entreviste al personal y revise la documentación para verificar que, al menos una vez cada 12 meses, el plan de respuesta a incidentes de seguridad es: • Revisado y actualizado según sea necesario. • Probado, incluyendo todos los elementos enumerados en el Requisito 12.10.1.	**Objetivo** Probar adecuadamente el plan de respuesta a incidentes de seguridad puede identificar procesos de negocios defectuosos y garantizar que no se pierdan pasos esenciales, lo que podría resultar en una mayor exposición durante un incidente. Las pruebas periódicas del plan aseguran que los procesos sigan siendo viables, al igual que garantizan que todo el personal relevante de la organización esté familiarizado con el plan. **Buenas Prácticas** La prueba del plan de respuesta a incidentes puede incluir incidentes simulados y las respuestas correspondientes en forma de “ejercicio de simulación”, que incluyan la participación del personal relevante. Una revisión del incidente y la calidad de la respuesta pueden brindar a las entidades la seguridad de que todos los elementos requeridos están incluidos en el plan.
Objetivo del Enfoque Personalizado El plan de respuesta a incidentes se mantiene actualizado y se prueba periódicamente.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **12.10.3** Se designa personal específico para estar disponible las 24 horas del día, los 7 días de la semana a fin de responder a incidentes de seguridad sospechosos o confirmados. **Objetivo del Enfoque Personalizado** Los incidentes se responden inmediatamente cuando corresponde.	**Procedimientos de Prueba de Enfoque Definido** **12.10.3** Evalúe la documentación y entreviste al personal responsable que ocupe los roles designados para verificar que el personal específico esté disponible las 24 horas del día, los 7 días de la semana para responder a incidentes de seguridad.	**Objetivo** Un incidente podría ocurrir en cualquier momento, por lo tanto, si una persona capacitada en respuesta a incidentes y que está familiarizada con el plan de la entidad está disponible cuando se detecta el incidente, la capacidad de la entidad para responder correctamente aumenta. **Buenas Prácticas** A menudo, se designa personal específico para formar parte de un equipo de respuesta a incidentes de seguridad, y el equipo tiene la responsabilidad general de responder a los incidentes (quizás en un horario rotativo) y gestionar esos incidentes de acuerdo con el plan. El equipo de respuesta a incidentes puede estar formado por miembros clave que están asignados de forma permanente, o por personal "a solicitud" que pueden ser llamados según sea necesario, según su experiencia y las características específicas del incidente. Tener recursos disponibles para responder rápidamente a los incidentes minimiza la interrupción del funcionamiento de la organización. Algunos ejemplos de tipos de actividad a los que el equipo, o las personas deben responder incluyen cualquier evidencia de actividad no autorizada, la detección de puntos de acceso inalámbrico no autorizados, alertas críticas de IDS e informes de cambios críticos no autorizados en el sistema o archivos de contenido.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **12.10.4** El personal responsable de responder a incidentes de seguridad sospechados y confirmados recibe capacitación adecuada y periódica sobre sus responsabilidades en la respuesta a incidentes. **Objetivo del Enfoque Personalizado** El personal conoce su función y responsabilidades en la respuesta a incidentes y puede obtener asistencia y orientación cuando sea necesario.	**Procedimientos de Prueba de Enfoque Definido** **12.10.4** Evalúe la documentación de capacitación y entreviste al personal de respuesta a incidentes para verificar que esté capacitado de manera adecuada y periódica acerca de sus responsabilidades de respuesta a incidentes.	**Objetivo** Sin un equipo de respuesta a incidentes capacitado y fácilmente disponible, podría ocurrir un daño extenso a la red, y los datos y sistemas críticos podrían “contaminarse” por el manejo inadecuado de los sistemas objetivo. Esto puede dificultar el éxito de una investigación posterior al incidente. **Buenas Prácticas** Es importante que todo el personal involucrado en la respuesta a incidentes esté capacitado y tenga conocimientos sobre el manejo de evidencia para análisis forense e investigaciones.
Requisitos del Enfoque Definido **12.10.4.1** La frecuencia de la capacitación periódica del personal de respuesta a incidentes es definida según el análisis de riesgos específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el requisito 12.3.1. **Objetivo del Enfoque Personalizado** El personal de respuesta a incidentes es entrenado con una frecuencia que aborda el riesgo de la entidad. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba de Enfoque Definido** **12.10.4.1.a** Evalúe el análisis de riesgos específico de la entidad en cuanto a la frecuencia de la capacitación del personal de respuesta a incidentes para verificar que el análisis de riesgos se haya sido realizado de acuerdo con todos los elementos especificados en el Requisito 12.3.1. **12.10.4.1.b** Evalúe los resultados documentados de la capacitación periódica del personal de respuesta a incidentes y entreviste al personal para verificar que la capacitación se realice con la frecuencia definida en el análisis de riesgos específico de la entidad realizado para este requisito.	**Objetivo** Los entornos y planes de respuesta a incidentes de cada entidad son diferentes, y el enfoque dependerá de una serie de factores, como el tamaño y la complejidad de la entidad, el grado de cambio en el entorno, el tamaño del equipo de respuesta a incidentes y la rotación del personal. La realización de un análisis de riesgos permitirá a la entidad determinar la frecuencia óptima para la formación del personal con responsabilidades de respuesta a incidentes.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
12.10.5 El plan de respuesta a incidentes de seguridad incluye el monitoreo y la respuesta a las alertas de los sistemas de monitoreo de seguridad, incluyendo, pero no limitado a: • Sistemas de detección y prevención de intrusiones. • Controles de seguridad de la red. • Mecanismos de detección de cambios en archivos críticos. • El mecanismo de detección de cambios y manipulaciones en las páginas de pago. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; consulte las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.* • Detección de puntos de acceso inalámbricos no autorizados.	**12.10.5** Evalúe la documentación y observe los procesos de respuesta a incidentes para verificar que el monitoreo y la respuesta a las alertas de los sistemas de monitoreo de seguridad están cubiertas en el plan de respuesta a incidentes de seguridad, incluyendo, pero no limitado a los sistemas especificados en este requerimiento.	Es esencial responder a las alertas generadas por los sistemas de monitoreo de la seguridad que están diseñados explícitamente para centrarse en el riesgo potencial para los datos a fin de impedir una infracción y, por lo tanto, esto debe incluirse en los procesos de respuesta a incidentes.
Objetivo del Enfoque Personalizado		
Las alertas generadas por las tecnologías de monitorización y detección se responden de forma estructurada y repetible.		
Notas de Aplicabilidad		
El punto anterior (para supervisar y responder a las alertas de un mecanismo de detección de cambios y manipulaciones para las páginas de pago) es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual se exigirá como parte del requisito 12.10.5 y deberá tenerse plenamente en cuenta durante una evaluación PCI DSS.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo** Incorporar las lecciones aprendidas en el plan de respuesta a incidentes después de que se produzca un incidente y al ritmo de la evolución del sector, ayuda a mantener el plan actualizado y con la capacidad de reaccionar ante las nuevas amenazas y tendencias de seguridad. **Buenas Prácticas** El ejercicio de lecciones aprendidas debe incluir todos los niveles del personal. Aunque a menudo se incluye como parte de la revisión de todo el incidente, este debe centrarse en cómo podría mejorarse la respuesta de la entidad al incidente. Es importante no sólo tener en cuenta los elementos de la respuesta que no tuvieron los resultados previstos, sino también comprender lo que funcionó bien y si las lecciones de esos elementos que funcionaron bien pueden aplicarse a las áreas del plan que no lo hicieron. Otra forma de optimizar el plan de respuesta a incidentes de una entidad es entender los ataques realizados contra otras organizaciones y utilizar esa información para afinar los procedimientos de detección, contención, mitigación o recuperación de la entidad.
12.10.6 El plan de respuesta a incidentes de seguridad se modifica y evoluciona de acuerdo con las lecciones aprendidas y para incorporar los desarrollos de la industria.	**12.10.6.a** Evalúe las políticas y procedimientos para verificar que los procesos están definidos a fin de modificar y evolucionar el plan de respuesta a incidentes de seguridad de acuerdo con las lecciones aprendidas e incorporar elementos de desarrollo de la industria.	
	12.10.6.b Evalúe el plan de respuesta a incidentes de seguridad y entreviste al personal responsable para verificar que el plan de respuesta a incidentes se modifica y evoluciona de acuerdo con las lecciones aprendidas, y para incorporar los desarrollos de la industria.	
Objetivo del Enfoque Personalizado		
La eficiencia y precisión del plan de respuesta a incidentes se revisa y actualiza después de cada invocación.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **12.10.7** Existen procedimientos de respuesta a incidentes que se iniciarán cuando se detecten datos de PAN almacenados en un lugar inesperado, e incluyen: • Determinar qué hacer si se descubren datos de PAN fuera del CDE, incluyendo su recuperación, eliminación segura y/o migración al CDE actualmente definido, según corresponda. • Identificar si los datos confidenciales de autenticación se almacenan con datos de PAN. • Determinar de dónde proceden los datos del tarjetahabiente y cómo han llegaron donde no se esperaba. • Remediar fugas de datos o brechas en el proceso que llevaron a que los datos del tarjetahabiente llegaran a una ubicación inesperada. **Objetivo del Enfoque Personalizado** Existen procesos para responder, analizar y abordar situaciones rápidamente en caso de que se detecten datos de PAN no cifrados en ubicaciones inapropiadas. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba de Enfoque Definido** **12.10.7.a** Evalúe los procedimientos de respuesta a incidentes documentados para verificar que los procedimientos para responder a la detección de datos de PAN almacenados en cualquier lugar inapropiado, estén listos para iniciarse e incluyan todos los elementos especificados en este requisito. **12.10.7.b** Entreviste al personal y estudiar los registros de las acciones de respuesta para verificar los procedimientos de respuesta, ante la detección de datos PAN almacenados en cualquier ubicación inapropiada.	**Objetivo** Contar con procedimientos documentados de respuesta a incidentes, que se cumplan en caso de que se encuentren datos de PAN almacenados en algún lugar donde no deberían estar, ayuda a identificar las acciones de remediación necesarias y a impedir fugas futuras. **Buenas Prácticas** Si se encuentran datos de PAN fuera del CDE, se debe realizar un análisis para 1) determinar si se guardaron independientemente de otros datos o con datos confidenciales de autenticación, 2) identificar la fuente de los datos, y 3) identificar las brechas de control que dieron lugar a que los datos estuvieran fuera del CDE. Las entidades deben considerar si existen factores que contribuyan, como procesos empresariales, comportamiento de los usuarios, configuraciones inadecuadas del sistema, etc., que hayan provocado que los datos de PAN se almacenasen en una ubicación inesperada. Si estos factores contribuyen con la situación, deben ser abordados según este requisito para evitar que se repitan.

Anexo A Requisitos Adicionales de PCI DSS

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

- Anexo A1: Requisitos Adicionales de PCI DSS para Proveedores de Servicios Multiusuario.
- Anexo A2: Requisitos Adicionales de PCI DSS Para Entidades que Utilizan SSL/Primeras Versiones de TLS para Conexiones de Terminal POS POI Presencial con Tarjetas.
- Anexo A3: Validación Suplementaria de Entidades Designadas (DESV).

En cada sección se proporciona información de orientación y aplicabilidad.

Anexo A1: Requisitos Adicionales de PCI DSS para Proveedores de Servicios Multiusuario

Secciones
A1.1 Los proveedores de servicios multiusuario protegen y separan todos los entornos y datos de los clientes.
A1.2 Los proveedores de servicios multiusuario facilitan el registro y la respuesta a incidentes para todos los clientes.

Descripción
Todos los proveedores de servicios son responsables de cumplir con los requisitos de PCI DSS para sus propios entornos según corresponda a los servicios ofrecidos a sus clientes. Además, los proveedores de servicios multiusuario deben cumplir con los requisitos de este Anexo.
Los proveedores de servicios multiusuario constituyen un tipo de proveedor de servicios de terceros que ofrece diversos servicios compartidos a comerciantes y otros proveedores de servicios, en los que los clientes comparten recursos del sistema (como servidores físicos o virtuales), infraestructura, aplicaciones (incluyendo el software como servicio (SaaS)) y/o bases de datos. Los servicios pueden incluir, entre otros, el alojamiento de múltiples entidades en un servidor único compartido, prestando servicios de comercio electrónico y/o "carrito de la compra", servicios de alojamiento basados en la web, aplicaciones de pago, diversas aplicaciones y servicios en la nube y conexiones a pasarelas y procesadores de pago.
Los proveedores de servicios que brindan solo servicios de centros de datos compartidos (a menudo llamados proveedores de ubicación conjunta o "co-lo"), donde el equipo, el espacio y el ancho de banda están disponibles bajo alquiler, no se consideran proveedores de servicios de multiusuario para los fines de este Anexo.
Nota: Aunque un proveedor de servicios multiusuario pueda cumplir con estos requisitos, cada cliente sigue siendo responsable de cumplir con los requisitos de PCI DSS que se aplican a su entorno y validar el cumplimiento según corresponda. A menudo existen requisitos de PCI DSS cuya responsabilidad se comparte entre el proveedor y el cliente (quizás para diferentes aspectos del entorno). Los requisitos 12.8 y 12.9 describen los requisitos específicos de las relaciones entre todos los proveedores de servicios externos (TPSP) y sus clientes, y las responsabilidades de ambos. Esto incluye definir los servicios específicos que recibe el cliente, junto con los requisitos de PCI DSS que el cliente tiene la responsabilidad de cumplir, cuáles son responsabilidad del TPSP y qué requisitos se comparten entre el cliente y el TPSP.

Requisitos y Procedimientos de Prueba		Guía
A1.1 Los proveedores de servicios multiusuario protegen y separan todos los entornos y datos de los clientes.		
Requisitos del Enfoque Definido **A1.1.1** La separación lógica se implementa de la siguiente manera: • El proveedor no puede ingresar a los entornos de sus clientes sin autorización. • Los clientes no pueden ingresar al entorno del proveedor sin autorización. **Objetivo del Enfoque Personalizado** Los clientes no pueden ingresar al entorno del proveedor. El proveedor no puede ingresar a los entornos de sus clientes sin autorización. **Notas de Aplicabilidad** *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*	**Procedimientos de Prueba de Enfoque Definido** **A1.1.1** Evalúe la documentación y las configuraciones del sistema y la red, y entreviste al personal para verificar que la separación lógica se implemente de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Sin controles entre el entorno del proveedor y el entorno del cliente, personas maliciosas dentro del entorno del proveedor podrían comprometer el entorno del cliente y, de manera similar, personas maliciosas en el entorno de un cliente, podría comprometer al proveedor y potencialmente a otros clientes del proveedor. Los entornos multiusuario deben estar aislados entre sí y de la infraestructura del proveedor de modo que puedan ser entidades administradas por separado sin conectividad entre ellas. **Buenas Prácticas** Los proveedores deben garantizar una fuerte separación entre los entornos que están diseñados para el acceso de los clientes, por ejemplo, los portales de configuración y facturación, y el entorno privado del proveedor al que solo debe ingresar el personal autorizado del proveedor. El acceso del proveedor de servicios a los entornos del cliente se realiza de acuerdo con el requisito 8.2.3. **Información Adicional** Refiérase a la *Información Complementaria:* Para mayor información sobre los entornos en la nube refiérase a *Directrices de Computación en la Nube PCI SCC.*

<table>
<tr><th colspan="2">Requisitos y Procedimientos de Prueba</th><th>Guía</th></tr>
<tr><td>Requisitos del Enfoque Definido</td><td>Procedimientos de Prueba de Enfoque Definido</td><td rowspan="3">Objetivo
Es importante que los proveedores de servicios multiusuario definan controles para que cada cliente solo pueda ingresar a su propio entorno y CDE para evitar el acceso no autorizado desde el entorno de un cliente a otro.
Ejemplos
En una infraestructura basada en la nube, como una infraestructura como servicio (IaaS), el CDE de los clientes puede incluir dispositivos de red virtual y servidores virtuales configurados y administrados por los clientes, incluidos sistemas operativos, archivos, memoria, etc.</td></tr>
<tr><td>A1.1.2 Los controles se implementan de modo que cada cliente solo tenga permiso para ingresar a sus propios datos de tarjetahabiente y CDE.</td><td>A1.1.2.a Evalúe la documentación para verificar que los controles estén definidos de manera que cada cliente solo tenga permiso para ingresar a sus propios datos de tarjetahabiente y CDE.</td></tr>
<tr><td>Objetivo del Enfoque Personalizado
Los clientes no pueden ingresar a los entornos de otros clientes.</td><td>A1.1.2.b Evalúe las configuraciones del sistema para verificar que los clientes tengan privilegios establecidos para ingresar solo a sus propios datos de cuenta y CDE.</td></tr>
<tr><td>Requisitos del Enfoque Definido</td><td>Procedimientos de Prueba de Enfoque Definido</td><td rowspan="3">Objetivo
Para evitar cualquier impacto involuntario o intencional en los entornos o datos de cuentas de otros clientes, es importante que cada cliente pueda ingresar solo a los recursos que le han sido asignados.</td></tr>
<tr><td>A1.1.3 Los controles se implementan de modo que cada cliente solo pueda ingresar a los recursos que se le han asignados.</td><td rowspan="2">A1.1.3 Evalúe los privilegios de los clientes para verificar que cada cliente solo pueda ingresar a los recursos que se le han asignado.</td></tr>
<tr><td>Objetivo del Enfoque Personalizado
Los clientes no pueden afectar los recursos asignados a otros clientes.</td></tr>
</table>

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
A1.1.4 La eficiencia de los controles de separación lógica utilizados para separar los entornos de los clientes se confirma al menos una vez cada seis meses mediante pruebas de penetración.	**A1.1.4** Evalúe los resultados de las pruebas de penetración más recientes para verificar que estas confirmaron la efectividad de los controles de separación lógica utilizados para separar los entornos de los clientes.	Los proveedores de servicios multiusuario son responsables de gestionar la segmentación entre sus clientes. Sin la garantía técnica de que los controles de segmentación son eficientes, es posible que los cambios en la tecnología del proveedor de servicios inadvertidamente generen una vulnerabilidad que podría ser explotada por todos los clientes del proveedor de servicios. **Buenas Prácticas** La eficiencia de las técnicas de separación se puede confirmar mediante el uso de entornos temporales (simulados) creados por el proveedor de servicios, que representan los entornos de los clientes, e intentando: 1) ingresar a un entorno temporal desde otro entorno e 2) ingresar a un entorno temporal desde Internet.
Objetivo del Enfoque Personalizado		
La segmentación de los entornos de clientes de otros entornos, se valida periódicamente para que sea eficiente.		
Notas de Aplicabilidad		
La prueba de separación adecuada entre los clientes en un entorno de proveedor de servicios multiusuario se suma a las pruebas de penetración especificadas en el Requisito 11.4.6. *Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
A1.2 Los proveedores de servicios multiusuario facilitan el registro y la respuesta a incidentes para todos los clientes.		
Requisitos del Enfoque Definido **A1.2.1** La función de registro de auditoría está habilitada para el entorno de cada cliente de conformidad con el Requisito 10 PCI DSS, que incluye lo siguiente: • Los registros están habilitados para aplicaciones comunes de terceros. • Los registros están activos de forma predeterminada. • Los registros están disponibles para revisión solo por parte del cliente propietario. • Las ubicaciones de los registros se comunican claramente al cliente propietario. • Los datos de registro y la disponibilidad son consistentes con el Requisito 10 PCI DSS. **Objetivo del Enfoque Personalizado** La función de registro está disponible para todos los clientes sin afectar la confidencialidad de otros clientes.	**Procedimientos de Prueba de Enfoque Definido** **A1.2.1** Evalúe la documentación y los ajustes de configuración del sistema para verificar que el proveedor haya habilitado la función de registro de auditoría para cada entorno de cliente, de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** La información de registro es útil para detectar y solucionar incidentes de seguridad y tiene un valor incalculable para las investigaciones forenses. Por lo tanto, los clientes deben tener acceso a estos registros. Sin embargo, la información de registro también puede ser utilizada por un atacante para el reconocimiento, por lo que la información del registro de un cliente sólo debe ser accesible por el cliente al que se refiere el registro.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **A1.2.2** Se implementan procesos o mecanismos para apoyar y/o facilitar investigaciones forenses rápidas en caso de un incidente de seguridad sospechado o confirmado para cualquier cliente.	**Procedimientos de Prueba de Enfoque Definido** **A1.2.2** Evalúe los procedimientos documentados para verificar que el proveedor tenga procesos o mecanismos para respaldar o facilitar una investigación forense rápida en los servidores relacionados, en caso de que se sospeche o se confirme un incidente de seguridad para cualquier cliente.	**Objetivo** En caso de que se sospeche o se confirme una violación de la confidencialidad de los datos de titulares de tarjetas, el investigador forense de un cliente tiene como objetivo encontrar la causa de la violación, expulsar al atacante del entorno y garantizar que se elimine todo acceso no autorizado. Las respuestas rápidas y eficientes a las solicitudes de los investigadores forenses pueden reducir significativamente el tiempo que tarda el investigador en proteger el entorno del cliente.
Objetivo del Enfoque Personalizado La investigación forense está disponible para todos los clientes en caso de sospecha o confirmación de un incidente de seguridad.		
Requisitos del Enfoque Definido **A1.2.3** Se implementan procesos o mecanismos para reportar y abordar vulnerabilidades e incidentes de seguridad presuntos o confirmados, incluyendo lo siguiente: • Los clientes pueden informar de forma segura los incidentes de seguridad y las vulnerabilidades al proveedor. • El proveedor aborda y repara los incidentes de seguridad y las vulnerabilidades sospechadas o confirmadas de acuerdo con el Requisito 6.3.1.	**Procedimientos de Prueba de Enfoque Definido** **A1.2.3** Evalúe los procedimientos documentados y entreviste al personal para verificar que el proveedor tenga un mecanismo para informar y abordar vulnerabilidades e incidentes de seguridad sospechados o confirmados, de acuerdo con todos los elementos especificados en este requisito.	**Objetivo** Las vulnerabilidades de seguridad en los servicios prestados pueden afectar la seguridad de todos los clientes del proveedor de servicios y, por lo tanto, deben gestionarse de acuerdo con los procesos establecidos por el proveedor de servicios, dando prioridad a la resolución de las vulnerabilidades que tienen la mayor probabilidad de compromiso. Es probable que los clientes noten vulnerabilidades y configuraciones incorrectas de seguridad mientras utilizan el servicio. La implementación de métodos seguros para que los clientes reporten incidentes de seguridad y vulnerabilidades, alienta a los clientes a reportar problemas potenciales y permite que el proveedor conozca y aborde rápidamente los problemas potenciales dentro de su entorno.
Objetivo del Enfoque Personalizado Se descubren y abordan vulnerabilidades o incidentes de seguridad sospechosos o confirmados. Cuando sea apropiado, los clientes son informados.		

Requisitos y Procedimientos de Prueba		Guía
Notas de Aplicabilidad		
Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.		

Anexo A2: Requisitos Adicionales de PCI DSS Para Entidades que Utilizan SSL/Primeras Versiones de TLS para Conexiones de Terminal POS POI Presencial con Tarjetas

Secciones
A2.1 Está confirmado que los terminales POI que utilizan SSL y/o primeras versiones de TLS no son susceptibles a las explotaciones conocidas de SSL/TLS.

Descripción

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

Las entidades que utilizan SSL y primeras versiones de TLS para las conexiones de terminales POS POI deben trabajar para actualizarse a un protocolo criptográfico sólido lo antes posible. Además, los protocolos SSL y/o primeras versiones de TLS no deben introducirse en entornos donde esos protocolos aún no existen. Al momento de esta publicación, las vulnerabilidades conocidas son difíciles de explotar en los terminales de pago POS POI. Sin embargo, podrían surgir nuevas vulnerabilidades en cualquier momento, y es responsabilidad de la organización mantenerse al día con las tendencias de vulnerabilidad y determinar si es susceptible a algún ataque conocido.

Los requisitos de PCI DSS directamente involucrados son:

- **Requisito 2.2.5**: Donde haya servicios, protocolos o demonios inseguros; se documenta la justificación empresarial y se documentan e implementan funciones de seguridad adicionales que reducen el riesgo de utilizar servicios, protocolos o demonios inseguros.
- **Requisito 2.2.7**: Todo el acceso administrativo sin consola está cifrado utilizando criptografía fuerte.
- **Requisito 4.2.1**: Se implementan protocolos de seguridad y criptografía fuerte para proteger los datos PAN durante la transmisión a través de redes públicas abiertas.

Los protocolos SSL y primeras versiones de TLS no deben usarse como control de seguridad para cumplir con estos requisitos, excepto en el caso de conexiones de terminales POS POI, como se detalla en este anexo. Para apoyar a las entidades que trabajan para migrar de SSL/primeras versiones de TLS a terminales POS POI, se incluyen las siguientes disposiciones:

- Las nuevas implementaciones de terminales POS POI no deben usar SSL o primeras versiones de TLS como control de seguridad.
- Todos los proveedores de servicios de terminales POS POI deben proveer una oferta de servicio segura.
- Los proveedores de servicios que admiten implementaciones de terminales POS POI existentes que usan SSL y/o primeras versiones de TLS deben contar con un Plan formal de Mitigación de Riesgos y Migración.
- Los terminales POS POI en entornos con tarjeta presente verificables, que no son susceptibles a ningún ataque conocido para SSL y primeras versiones de TLS, **y los puntos de terminación de SSL/TLS a los que se conectan**, pueden continuar utilizando SSL/Primeras versiones de TLS como control de seguridad.

Los Requisitos en este Anexo no son aptos para el Enfoque Personalizado.

Requisitos y Procedimientos de Prueba		Guía
A2.1 Está confirmado que Los terminales POI que utilizan SSL y/o versiones iniciales de TLS no son susceptibles a explotaciones conocidas de SSL/TLS.		
Requisitos del Enfoque Definido **A2.1.1** Cuando los terminales POS POI en el comercio o en la ubicación de aceptación de pagos usan SSL y/o primeras versiones de, la entidad confirma que los dispositivos no son susceptibles a ninguna vulnerabilidad conocida para esos protocolos. **Objetivo del Enfoque Personalizado** Este requisito no es elegible para el enfoque personalizado. **Notas de Aplicabilidad** Este requisito está destinado a aplicarse a la entidad con el terminal POS POI, como un comerciante. Este requisito no está destinado a los proveedores de servicios que sirven como punto de terminación o conexión a esos terminales POS POI. Los requisitos A2.1.2 y A2.1.3 se aplican a los proveedores de servicios POS POI. La asignación para terminales POS POI que actualmente no son susceptibles a vulnerabilidades se basa en los riesgos actualmente conocidos. Si se introducen nuevas vulnerabilidades a las que los terminales POS POI son susceptibles, estas deberán actualizarse inmediatamente.	**Procedimientos de Prueba de Enfoque Definido** **A2.1.1** Para terminales POS POI que utilizan SSL o primeras versiones de TLS, confirme que la entidad tiene documentación (por ejemplo, documentación del proveedor, detalles de la configuración del sistema o de la red) que verifica que los dispositivos no son susceptibles a vulnerabilidades conocidas para SSL/primeras versiones de TLS.	**Objetivo** Los terminales POS POI utilizados en entornos con tarjeta presente pueden continuar usando SSL/primeras versiones de TLS cuando se puede demostrar que el terminal POS POI no es susceptible a las vulnerabilidades actualmente conocidas. **Buenas Prácticas** Sin embargo, SSL es una tecnología obsoleta y podría ser susceptible a vulnerabilidades de seguridad adicionales en el futuro; por lo tanto, se recomienda enfáticamente que los terminales POS POI se actualicen a un protocolo seguro lo antes posible. Si no se necesita SSL/primeras versiones de TLS en el entorno, se debe deshabilitar el uso y el apoyo de estas versiones. **Información Adicional** Consulte los Suplementos de información actualizados PCI SCC sobre SSL/primeras versiones de TLS para obtener más orientación.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
A2.1.2 ***Requisito solo para proveedores de servicios:*** Todos los proveedores de servicios con puntos de conexión existentes POS POI que utilizan SSL y/o primeras versiones de TLS como se define en A2.1 cuentan con un Plan de Migración y Mitigación de Riesgos que incluye: • Descripción del uso, incluidos los datos que se transmiten, los tipos y la cantidad de sistemas que usan y/o admiten SSL/primeras versiones de TLS y el tipo de entorno. • Resultados de la evaluación de riesgos y controles de reducción de riesgos implementados. • Descripción de procesos para monitorear nuevas vulnerabilidades relacionadas con SSL/primeras versiones de TLS. • Descripción de los procesos de control de cambios que se implementan para garantizar que los SSL/primeras versiones de TLS no se implementen en nuevos entornos. • Descripción general del plan del proyecto de migración para reemplazar los SSL/primeras versiones de TLS en una fecha futura.	**A2.1.2** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Revise el Plan de Mitigación de Riesgos y Migración documentado para verificar que incluya todos los elementos especificados en este requisito.	Los puntos de terminación POI POS, incluyendo, entre otros, proveedores de servicios como adquirientes o procesadores de adquirientes, pueden continuar utilizando SSL/primeras versiones de TLS cuando se pueda demostrar que el proveedor de servicios cuenta con controles que mitigan el riesgo de apoyar esas conexiones para el entorno del proveedor de servicios. **Buenas Prácticas** Los proveedores de servicios deben comunicar a todos los clientes que utilizan SSL/primeras versiones de TLS acerca de los riesgos asociados con su uso y la necesidad de migrar a un protocolo seguro. **Definiciones** El Plan de Mitigación de Riesgos y Migración es un documento preparado por la entidad que detalla sus planes para migrar a un protocolo seguro y describe los controles que la entidad tiene implementados para reducir el riesgo asociado con SSL/primeras versiones de TLS hasta que se complete la migración. **Información Adicional** Consulte los Suplementos de información PCI SSC actuales sobre SSL/primeras versiones de TLS para obtener más orientación sobre los Planes de Migración y Mitigación de Riesgos.
Objetivo del Enfoque Personalizado Este requisito no es elegible para el enfoque personalizado.		
Notas de Aplicabilidad Este requisito se aplica solo cuando la entidad evaluada es un proveedor de servicios.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido **A2.1.3** Requisito Solo Para Proveedores de Servicios: Todos los proveedores de servicios brindan una oferta de servicios segura. **Objetivo del Enfoque Personalizado** Este requisito no es elegible para el enfoque personalizado. **Notas de Aplicabilidad** Este requisito se aplica solo cuando la entidad evaluada es un proveedor de servicios.	**Procedimientos de Prueba de Enfoque Definido** **A2.1.3** ***Procedimiento de prueba adicional solo para evaluaciones de proveedores de servicios:*** Evalúe las configuraciones del sistema y la documentación de apoyo para verificar que el proveedor de servicios ofrezca una opción de protocolo seguro para su servicio.	**Objetivo** Los clientes deben poder optar por actualizar sus POI para eliminar la vulnerabilidad al usar SSL y primeras versiones de TLS. En muchos casos, los clientes deberán adoptar un enfoque por etapas o gradual para migrar su estado POS POI del protocolo inseguro a un protocolo seguro y, por lo tanto, requerirán que el proveedor de servicios respalde una oferta segura. **Información Adicional** Consulte los Suplementos de información actualizados PCI SCC sobre SSL/primeras versiones de TLS para obtener más orientación.

Anexo A3: Validación Complementaria de Entidades Designadas (DESV)

Secciones
A3.1 Se implementa un programa de cumplimiento PCI DSS.
A3.2 El alcance PCI DSS está documentado y validado.
A3.3 PCI DSS se incorporan a las actividades habituales (BAU).
A3.4 El acceso lógico al entorno de datos de titulares de la tarjeta, se controla y gestiona.
A3.5 Los eventos sospechosos son identificados y respondidos.

Descripción

Este anexo se aplica solo a las entidades designadas por una(s) franquicia(s) de pago o adquirentes que requieren una validación adicional de los requisitos vigentes PCI DSS. Se requiere que la entidad se someta a una evaluación de acuerdo con este Anexo ÚNICAMENTE si se lo indica un adquirente o una franquicia de pago. Ejemplos de entidades a las que podría aplicarse este Anexo incluyen:

- Los que almacenan, procesan o transmiten grandes volúmenes de datos de cuentas,
- Aquellos que proporcionan puntos de agregación para datos de cuentas, o
- Aquellos que hayan sufrido violaciones significativas o reiteradas de los datos de cuentas.

Además, otros estándares PCI pueden hacer referencia a la finalización de este Anexo.

Estos pasos de validación complementarios están destinados a brindar una mayor garantía de que los controles PCI DSS se mantienen de manera eficiente y continua a través de la validación de los procesos habituales (BAU) y una mayor consideración de validación y alcance.

***Nota**: Algunos requisitos tienen plazos definidos (por ejemplo, al menos una vez cada tres meses o al menos una vez cada seis meses) dentro de los cuales se deben realizar ciertas actividades. Para la evaluación inicial de este documento, no se requiere que se haya realizado una actividad por cada período de tiempo durante el año anterior, si el asesor verifica:*

- *La actividad se ha realizado de acuerdo con el requisito aplicable dentro del lapso más reciente (por ejemplo, el período de tres o seis meses más recientes), y*
- *La entidad cuenta con políticas y procedimientos documentados para seguir realizando la actividad dentro del plazo definido.*

Para los años posteriores a la evaluación inicial, se debe haber realizado una actividad dentro de cada período de tiempo requerido (por ejemplo, una actividad requerida cada tres meses debe haberse realizado al menos cuatro veces durante el año anterior en un intervalo que no exceda los 90 días).

No todos los requisitos de PCI DSS se aplican a todas las entidades que pueden someterse a una evaluación PCI DSS. Es por esta razón que algunos requisitos de PCI DSS se duplican en este anexo. Cualquier pregunta sobre este anexo debe dirigirse a los adquirentes o marcas de pago.

Requisitos y Procedimientos de Prueba		Guía
A3.1 Se implementa un programa de cumplimiento de PCI DSS.		
Requisitos del Enfoque Definido **A3.1.1** La responsabilidad es establecida por la gerencia ejecutiva para la protección de datos de titulares de tarjetas y un programa de cumplimiento PCI DSS que incluye: • Responsabilidad general para mantener el cumplimiento PCI DSS. • Definición de un estatuto para un programa de cumplimiento PCI DSS. • Proporcionar actualizaciones a la gerencia ejecutiva y a la junta directiva con iniciativas y problemas de cumplimiento PCI DSS, incluidas las actividades de remediación, al menos una vez cada 12 meses. **Términos de Referencia PCI DSS**: *Requisito 12* **Objetivo del Enfoque Personalizado** Este requisito no es elegible para el enfoque personalizado.	**Procedimientos de Prueba de Enfoque Definido** **A3.1.1.a** Evalúe la documentación para verificar que la gerencia ejecutiva haya asignado la responsabilidad general de mantener el cumplimiento PCI DSS de la entidad. **A3.1.1.b** Evalúe los estatutos PCI DSS de la empresa para verificar que describen las condiciones bajo las cuales se organiza el programa de cumplimiento PCI DSS. **A3.1.1.c** Evalúe las minutas y/o presentaciones de las reuniones de la gerencia ejecutiva y de la junta directiva para garantizar que las iniciativas de cumplimiento PCI DSS y las actividades de remediación se comuniquen al menos una vez cada 12 meses.	**Objetivo** La asignación que hace la gerencia ejecutiva de las responsabilidades de cumplimiento PCI DSS, garantiza la visibilidad, a nivel ejecutivo, del programa de cumplimiento PCI DSS y brinda la oportunidad de generar las preguntas adecuadas para determinar la eficiencia del programa e influir en las prioridades estratégicas. **Buenas Prácticas** La dirección ejecutiva puede incluir puestos de nivel C, junta directiva o equivalente. Los títulos específicos dependerán de la estructura organizacional particular. La responsabilidad del programa de cumplimiento PCI DSS se puede asignar a roles individuales y/o a unidades de negocios dentro de la organización.

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
A3.1.2 Existe un programa formal de cumplimiento PCI DSS que incluye: • Definición de las actividades para mantener y supervisar el cumplimiento general PCI DSS, incluidas las actividades habituales. • Procesos de evaluación anual PCI DSS. • Procesos para la validación continua de los requisitos de PCI DSS (por ejemplo, diariamente, semanalmente, cada tres meses, según corresponda según el requisito). • Un proceso para realizar un análisis del impacto en el negocio para determinar los posibles impactos PCI DSS en las decisiones estratégicas del negocio. **Términos de Referencia PCI DSS**: *Requisitos 1-12*	**A3.1.2.a** Evalúe las políticas y procedimientos de seguridad de la información para verificar que los procesos están definidos para un programa formal de cumplimiento PCI DSS que incluya todos los elementos especificados en este requisito. **A3.1.2.b** Entreviste al personal y observe las actividades de cumplimiento para verificar que se implemente un programa formal de cumplimiento PCI DSS de acuerdo con todos los elementos especificados en este requisito.	Un programa de cumplimiento formal permite a la organización monitorear el estado de sus controles de seguridad, ser proactivo ante fallas, y comunicar de manera efectiva las actividades y el estado de cumplimiento en toda la organización. **Buenas Prácticas** El programa de cumplimiento PCI DSS puede ser un programa especializado o ser parte de un programa general de cumplimiento y/o gobernanza, y debe incluir una metodología bien definida que demuestre una evaluación coherente y eficiente. Las decisiones empresariales estratégicas que deben analizarse para detectar posibles impactos PCI DSS pueden incluir fusiones y adquisiciones, nuevas compras de tecnología o nuevos canales de aceptación de pagos. **Definiciones** El mantenimiento y el monitoreo del cumplimiento general PCI DSS por parte de una organización incluye la identificación de las actividades que deben llevarse a cabo diariamente, semanalmente, mensualmente, cada tres meses o anualmente, y la garantía de que estas actividades se están llevando a cabo de manera consecuente (por ejemplo, utilizando una metodología de autoevaluación de la seguridad o PDCA). **Ejemplos** Las metodologías que apoyan la gestión de los programas de cumplimiento incluyen *Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC y Six Sigma.*
Objetivo del Enfoque Personalizado		
Este requisito no es elegible para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
A3.1.3 Los roles y responsabilidades de cumplimiento PCI DSS se definen de forma específica y se asignan formalmente a uno o más miembros del personal, incluyendo: • Gestionar las actividades habituales PCI DSS. • Gestionar los procesos de evaluación anual PCI DSS. • Gestionar los procesos para la validación continua de los requisitos de PCI DSS (por ejemplo, diariamente, semanalmente, cada tres meses, según corresponda según el requisito). • Gestionar un proceso para realizar un análisis del impacto en el negocio para determinar los posibles impactos PCI DSS en las decisiones estratégicas del negocio. **Términos de Referencia PCI DSS**: *Requisito 12*	**A3.1.3.a** Evalúe las políticas y procedimientos de seguridad de la información y entreviste al personal para verificar que los roles y responsabilidades de cumplimiento PCI DSS están específicamente definidas y formalmente asignadas a uno o más miembros del personal de acuerdo con todos los elementos de este requisito.	La definición formal de los roles y responsabilidades de cumplimiento específicas PCI DSS ayuda a garantizar la rendición de cuentas y el monitoreo continuo de los esfuerzos de cumplimiento PCI DSS. **Buenas Prácticas** La propiedad debe asignarse a personas con autoridad para tomar decisiones basadas en el riesgo y sobre las que recaiga la responsabilidad de la función específica. Las funciones deben estar formalmente definidas y los propietarios deben ser capaces de demostrar que comprenden sus responsabilidades y su obligación de rendir cuentas. Las funciones de cumplimiento pueden asignarse a un único propietario o a varios propietarios para diferentes elementos de los requisitos.
Objetivo del Enfoque Personalizado	**A3.1.3.b** Entreviste al personal responsable y verificar que está familiarizado con sus responsabilidades de cumplimiento PCI DSS y que las están desempeñando.	
Este requisito no es elegible para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo** Para poder desempeñar su función, el personal responsable del cumplimiento PCI DSS tiene necesidades específicas de formación que superan a las que suele incluir la formación general de concienciación en materia de seguridad. **Buenas Prácticas** Las personas con responsabilidades de cumplimiento PCI DSS deben recibir una formación especializada que, además de concientización general sobre seguridad de la información, se centre en los temas, habilidades, procesos o metodologías de seguridad específicos que deben seguirse, para que dichas personas puedan desempeñar sus responsabilidades de cumplimiento de forma eficiente. La capacitación puede ser ofrecida a lo interno o por terceros, como para PCI SCC (por ejemplo, concienciación PCI, PCIP e ISA), marcas de pago y adquirientes. El contenido de la capacitación debe ser aplicable a la función laboral del individuo, estar actualizada e incluir las últimas amenazas a la seguridad y/o la versión PCI DSS más reciente. **Información Adicional** Para obtener orientación adicional, refiérase a la *Información Complementaria: Mejores Prácticas para Implementar un Programa de* concienciación *sobre la Seguridad*.
A3.1.4 La formación actualizada sobre PCI DSS y/o seguridad de la información se imparte al menos una vez cada 12 meses y está dirigida al personal con responsabilidades de cumplimiento PCI DSS (como se identifica en A3.1.3). **Términos de Referencia PCI DSS**: *Requisito 12*	**A3.1.4.a** Evalúe las políticas y los procedimientos de seguridad de la información para verificar que la capacitación en materia PCI DSS y/o seguridad de la información es necesaria al menos una vez cada 12 meses para cada función con responsabilidades de cumplimiento PCI DSS.	
Objetivo del Enfoque Personalizado Este requisito no es elegible para el enfoque personalizado.	**A3.1.4.b** Entreviste al personal y evalúe los certificados de asistencia u otros registros para verificar que el personal con responsabilidad de cumplimiento PCI DSS recibe capacitación actualizada sobre PCI DSS y/o seguridad de la información o similar al menos una vez cada 12 meses.	

Requisitos y Procedimientos de Prueba		Guía
A3.2 El alcance PCI DSS está documentado y validado.		
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	
A3.2.1 El alcance PCI DSS es documentado y su precisión confirmada por la entidad al menos una vez cada tres meses y ante cambios significativos en el entorno dentro del alcance. Como mínimo, la validación del alcance incluye: • Identificar todos los flujos de datos para las diversas etapas de pago (por ejemplo, autorización, captura, liquidación, devoluciones y reembolsos) y canales de aceptación (por ejemplo, tarjeta física, tarjeta virtual y comercio electrónico). • Actualizar todos los diagramas de flujo de datos según el Requisito 1.2.4. • Identificar todas las ubicaciones en las que se almacenan, procesan y transmiten datos de cuentas, incluyendo, pero sin limitarse a ello, 1) cualquier locación fuera del CDE actualmente definida, 2) aplicaciones que procesan CHD, 3) transmisiones entre sistemas y redes, y 4) copias de seguridad de archivos. • Para cualquier dato de cuenta que se encuentre fuera del CDE actualmente definido, 1) elimínelo de forma segura, 2) migrarlo al CDE actualmente definido, o 3) ampliar el CDE actualmente definido para incluirlo. • Identificar todos los componentes del sistema en el CDE, conectados al CDE o que podrían afectar la seguridad del CDE. • Identificar todos los controles de segmentación en uso y los entornos desde los que se segmenta el CDE, incluida la justificación de los entornos que están fuera del alcance. *(continúa en la página siguiente)*	**A3.2.1.a** Evalúe los resultados documentados de las revisiones del alcance y entreviste al personal para verificar que se realicen las revisiones: • Al menos una vez cada tres meses. • Después de cambios significativos en el entorno dentro del alcance.	**Objetivo** La validación frecuente del alcance PCI DSS ayuda a garantizar que el alcance PCI DSS permanezca actualizado y alineado con los objetivos de negocios cambiantes y, por lo tanto, que los controles de seguridad protejan todos los componentes apropiados del sistema. **Buenas Prácticas** El alcance preciso implica evaluar críticamente el CDE y todos los componentes del sistema conectado para determinar la cobertura necesaria para los requisitos de PCI DSS. Las actividades de alcance, incluido el análisis detallado y el monitoreo continuo, ayudan a garantizar que los sistemas dentro del alcance estén debidamente protegidos. Al documentar las ubicaciones de los datos de la cuenta, la entidad puede considerar crear una tabla u hoja de cálculo que incluya la siguiente información: • Almacenamiento de datos (bases de datos, archivos, nube, etc.), incluyendo el propósito del almacenamiento de datos y el período de retención, • Qué elementos de CHD se almacenan (datos PAN, fecha de caducidad, nombre del titular de la tarjeta y/o cualquier elemento de SAD antes de completar la autorización), • Cómo se protegen los datos (tipo de cifrado y robustez, algoritmo de *hash* y robustez, truncamiento, tokenización), • Cómo se registra el acceso a las bodegas de datos, incluyendo una descripción de los mecanismos de registro en uso (solución empresarial, nivel de aplicación, nivel de sistema operativo, etc.). *(continúa en la página siguiente)*

Requisitos y Procedimientos de Prueba		Guía
• Identificar todas las conexiones de entidades de terceros con acceso al CDE. • Confirmar que todos los flujos de datos identificados, datos de cuentas, componentes del sistema, controles de segmentación y conexiones de terceros con acceso al CDE están incluidos en el alcance. **Términos de Referencia PCI DSS**: *Alcance de los Requisitos de PCI DSS; Requisitos 12.*	**A3.2.1.b** Evalúe los resultados documentados de las revisiones del alcance que se producen al menos una vez cada tres meses para verificar que la validación del alcance incluye todos los elementos especificados en este requisito.	Además de los sistemas y redes internos, todas las conexiones de entidades de terceros, por ejemplo, socios de negocios, entidades que brindan servicios de apoyo remoto y otros proveedores de servicios, deben identificarse para determinar la inclusión en el alcance PCI DSS. Una vez que se han identificado las conexiones dentro del alcance, se pueden implementar los controles PCI DSS aplicables para reducir el riesgo de que se utilice una conexión de terceros para comprometer al CDE de una entidad. Se puede usar una herramienta o metodología de descubrimiento de datos para facilitar la identificación de todas las fuentes y ubicaciones de datos PAN, y para buscar datos PAN que residen en sistemas y redes fuera del CDE definido actualmente o en lugares inesperados dentro del CDE definido, por ejemplo, en un registro errado o en un archivo de volcado de memoria. Este enfoque puede ayudar a garantizar que se detecten ubicaciones previamente desconocidas de datos PAN y que los datos PAN se eliminen o se aseguren adecuadamente. **Información Adicional** Refiérase a la *Información Complementaria: Orientación para el Alcance y la Segmentación de Red PCI DSS* para obtener orientación adicional. *de Red PCI DSS* para obtener orientación adicional.
Objetivo del Enfoque Personalizado Este requisito no es elegible para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo**
A3.2.2 Se determina el impacto del alcance PCI DSS para todos los cambios en los sistemas o redes, incluyendo las adiciones de nuevos sistemas y nuevas conexiones de red. Los procesos incluyen: • Realizar una evaluación formal del impacto PCI DSS. • Identificar los requisitos de PCI DSS aplicables al sistema o a la red. • Actualizar el alcance PCI DSS según corresponda. • Aprobación documentada de los resultados de la evaluación de impacto por parte del personal responsable (como se define en A3.1.3). **Términos de Referencia PCI DSS**: *Alcance de los Requisitos de PCI DSS; Requisitos 1-12*	**A3.2.2** Evalúe la documentación de los cambios y entrevistar al personal para verificar que, para cada cambio en los sistemas o redes, se determine el impacto al alcance PCI DSS e incluya todos los elementos especificados en este requisito.	Los cambios en los sistemas o en las redes pueden tener un impacto significativo en el ámbito PCI DSS. Por ejemplo, los cambios en las reglas de control de seguridad de la red pueden hacer que segmentos enteros de la red entren en el ámbito de aplicación, o pueden añadirse nuevos sistemas al CDE, los cuales deben protegerse apropiadamente. Una evaluación formal del impacto realizada antes de un cambio, brinda a la entidad la garantía de que el cambio no afectará negativamente la seguridad del CDE. **Buenas Prácticas** Los procesos para determinar el impacto potencial que los cambios en los sistemas y redes pueden tener en el ámbito PCI DSS de una entidad, pueden desempeñarse como parte de un programa de cumplimiento PCI DSS específico, o pueden formar parte del programa general de cumplimiento y/o de gobernanza de la entidad.
Objetivo del Enfoque Personalizado		
Este requisito no es elegible para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos del Enfoque Definido	**Procedimientos de Prueba de Enfoque Definido**	**Objetivo** Es importante contar con procesos para analizar todos los cambios realizados en los sistemas o las redes, a fin de garantizar que se apliquen todos los controles PCI DSS apropiados a cualquier sistema o red que se añada al entorno en cuestión, como resultado de un cambio. La incorporación de esta validación en los procesos de gestión de cambios ayuda a garantizar que los inventarios de dispositivos y los estándares de configuración se mantengan actualizados y que se apliquen controles de seguridad donde sea necesario. **Buenas Prácticas** Un proceso de gestión de cambios debe incluir pruebas que demuestren que los requisitos de PCI DSS se aplican o se conservan mediante un proceso reiterativo. **Ejemplos** Los requisitos de PCI DSS que deben verificarse incluyen, entre otros, los siguientes: • Los diagramas de red se actualizan para reflejar los cambios. • Los sistemas se configuran según los estándares de configuración, con todas las contraseñas predeterminadas cambiadas y los servicios innecesarios deshabilitados. • Los sistemas están protegidos con los controles necesarios, por ejemplo, monitoreo de la integridad de los archivos, antimalware, parches y registro de auditoría. • Los datos confidenciales de autenticación no se almacenan, y todo el almacenamiento de datos de cuentas está documentado e incorporado en la política y los procedimientos de retención de datos. *(continúa en la página siguiente)*
A3.2.2.1 Tras la realización de un cambio, se confirma que todos los requisitos relevantes PCI DSS se son implementados en todos los sistemas y redes nuevas o modificadas, y se actualiza la documentación según corresponda. **Términos de Referencia PCI DSS**: *Alcance de los Requisitos de PCI DSS; Requisitos 1-12*	**A3.2.2.1** Evalúe los registros de cambios y los sistemas/redes afectados y entreviste al personal para verificar que se confirmó la implementación de todos los requisitos pertinentes PCI DSS y la actualización de la documentación como parte del cambio.	
Objetivo del Enfoque Personalizado		
Este requisito no es apto para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
		• Los nuevos sistemas se incluyen en el proceso de análisis de vulnerabilidades trimestral.
Requisitos de Enfoques Definidos **A3.2.3** Los cambios en la estructura organizacional dan como resultado una revisión formal (interna) del impacto en el alcance PCI DSS y la aplicabilidad de los controles. **Términos de Referencia PCI DSS**: *Requisito 12* **Objetivo del Enfoque Personalizado** Este requisito no es apto para el enfoque personalizado.	**Procedimientos de Prueba del Enfoque Definido** **A3.2.3** Evalúe las políticas y procedimientos para verificar que un cambio en la estructura organizacional involucre una revisión formal del impacto en el alcance y la aplicabilidad de los controles PCI DSS.	**Propósito** La estructura y la gestión de una organización definen los requisitos y el protocolo para operaciones eficientes y seguras. Los cambios en esta estructura podrían tener efectos negativos en los controles y marcos existentes al reasignar o eliminar recursos que alguna vez respaldaron los controles PCI DSS o al heredar nuevas responsabilidades que pueden no tener controles establecidos. Por lo tanto, es importante revisar el alcance y los controles PCI DSS cuando haya cambios en la estructura y administración de una organización para garantizar que los controles estén implementados y activos. **Ejemplos** Los cambios en la estructura organizativa incluyen, entre otros, fusiones o adquisiciones de empresas y cambios significativos o reasignaciones de personal responsable de los controles de seguridad.

Requisitos y Procedimientos de Prueba		Guía
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** PCI DSS normalmente requiere que los controles de segmentación se verifiquen mediante pruebas de penetración cada doce meses. Es probable que la validación de los controles de segmentación más frecuentemente revele fallas en la segmentación antes de que estas puedan ser aprovechadas por un atacante quien intente pivotar lateralmente desde una red no confiable fuera del alcance al CDE. **Buenas Prácticas** Aunque el requisito especifica que esta validación del alcance se desarrolla al menos una vez cada seis meses y después de un cambio significativo, este ejercicio debe desarrollarse lo más frecuentemente posible para garantizar que siga siendo eficiente para aislar el CDE de otras redes. **Información Adicional** Refiérase a la *Información Complementaria: Guía de Pruebas de Penetración* para orientación adicional.
A3.2.4 Si se utiliza la segmentación, el alcance PCI DSS se confirma de la siguiente manera: • Según la metodología de la entidad definida en el Requisito 11.4.1. • Las pruebas de penetración se realizan en los controles de segmentación al menos una vez cada seis meses y después de cualquier cambio en los controles/métodos de segmentación. • La prueba de penetración cubre todos los controles/métodos de segmentación en uso. • La prueba de penetración verifica que los controles/métodos de segmentación sean operativos y eficientes, y que aíslen el CDE de todos los sistemas fuera del alcance. **Términos de Referencia PCI DSS**: *Requisito 11*	**A3.2.4** Evalúe los resultados de la prueba de penetración más reciente para verificar que se haya realizado de acuerdo con todos los elementos especificados en este requisito.	
Objetivo del Enfoque Personalizado		
Este requisito no es apto para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** PCI DSS requiere que, como parte del ejercicio de su alcance, las entidades evaluadas deben identificar y documentar la existencia de todos los datos PAN no cifrados en sus entornos. Implementar una metodología de localización de datos que identifique todas las fuentes y ubicaciones de datos PAN no cifrados y busque datos PAN no cifrados en sistemas y redes fuera del CDE definido actualmente o en lugares inesperados dentro del CDE definido, por ejemplo, en un registro de errores o en un archivo de volcado de memoria, ayuda a garantizar que las ubicaciones previamente desconocidas de datos PAN no cifrados se detecten y protejan adecuadamente. **Ejemplos** Un proceso de localización de datos se puede realizar a través de una variedad de métodos, incluyendo, entre otros, 1) software de localización de datos disponible comercialmente, 2) un programa de localización de datos desarrollado internamente o 3) una búsqueda manual. También se puede utilizar una combinación de metodologías según sea necesario. Independientemente del método utilizado, el objetivo del esfuerzo es encontrar todas las fuentes y ubicaciones de datos PAN no cifrados (no solamente en el CDE definido).
A3.2.5 Se implementa una metodología de localización de datos que: • Confirma el alcance PCI DSS. • Ubica todas las fuentes y ubicaciones de datos PAN no cifrados al menos una vez cada tres meses y ante cambios significativos en el CDE o los procesos. • Aborda la posibilidad de que datos PAN no cifrados residan en sistemas y redes fuera del CDE definido actualmente. **Términos de Referencia PCI DSS**: *Alcance de los requisitos de PCI DSS*	**A3.2.5.a** Evalúe la metodología de localización de datos documentada para verificar que incluye todos los elementos especificados en este requisito. **A3.2.5.b** Evalúe los resultados de los esfuerzos recientes de localización de datos y entreviste al personal responsable para verificar que la localización de datos se realice al menos una vez cada tres meses y ante cambios significativos en el CDE o en los procesos.	
Objetivo del Enfoque Personalizado Este requisito no es elegible para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
A3.2.5.1 Los métodos de localización de datos se confirman de la siguiente manera: • Se prueba la eficiencia de los métodos. • Los métodos pueden descubrir datos PAN no cifrados en todos los tipos de componentes del sistema y formatos de archivo en uso. • La eficiencia de los métodos de localización de datos se confirma al menos una vez cada 12 meses. **Términos de Referencia PCI DSS**: *Alcance de los requisitos de PCI DSS*	**A3.2.5.1.a** Entreviste al personal y revise la documentación para verificar lo siguiente: • La entidad cuenta con un proceso para probar la eficiencia de los métodos utilizados para la localización de datos. • El proceso incluye la verificación de los métodos que pueden descubrir datos PAN no cifrados en todos los tipos de componentes del sistema y formatos de archivo en uso.	Un proceso para probar la eficiencia de los métodos utilizados para la localización de datos garantiza la integridad y precisión de la detección de datos de cuentas. **Buenas Prácticas** Para completar, los componentes del sistema en las redes dentro del alcance y los sistemas en las redes fuera del alcance deben incluirse en el proceso de localización de datos. El proceso de localización de datos debe ser eficiente en todos los sistemas operativos y plataformas en uso. La precisión se puede probar colocando datos PAN de prueba en componentes del sistema y formatos de archivo en uso y confirmando que el método de localización de datos detectó los datos PAN de prueba.
Objetivo del Enfoque Personalizado Este requisito no es apto para el enfoque personalizado.	**A3.2.5.1.b** Evalúe los resultados de las pruebas de eficiencia para verificar que la eficiencia de los métodos de localización de datos se confirme al menos una vez cada 12 meses.	
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
A3.2.5.2 Se implementan procedimientos de respuesta ante la detección de datos PAN no cifrados fuera del CDE que incluyen: *(continúa en la página siguiente)*	**A3.2.5.2.a** Evalúe los procedimientos de respuesta documentados para verificar que los procedimientos para responder a la detección de datos PAN no cifrados fuera del CDE estén definidos e incluyan todos los elementos especificados en este requisito.	Aplicar procedimientos de respuesta documentados en caso de que se encuentren datos PAN no cifrados fuera del CDE, ayuda a identificar las soluciones necesarias e impedir fugas futuras.

Requisitos y Procedimientos de Prueba		Guía
• Determinar qué hacer si se descubren datos PAN fuera del CDE, incluyendo su recuperación, eliminación segura y/o migración al CDE actualmente definido, según corresponda. • Determinar cómo los datos terminaron fuera del CDE. • Remediar fugas de datos o brechas en el proceso que llevaron a que los datos llegaran a una ubicación fuera del CDE. • Identificar la fuente de los datos. • Identificar si se almacenan datos de track con los datos PAN. **Objetivo del Enfoque Personalizado** Este requisito no es apto para el enfoque personalizado.	**A3.2.5.2.b** Entreviste al personal y Evalúelos registros de las acciones de respuesta para verificar que se lleven a cabo las actividades correctivas cuando se detectan datos PAN fuera del CDE.	**Buenas Prácticas** Si se encuentran datos PAN fuera del CDE, se debe realizar un análisis para 1) determinar si se guardaron independientemente de otros datos o con datos confidenciales de autenticación, 2) identificar la fuente de los datos, y 3) identificar las brechas de control que dieron lugar a que los datos estuvieran fuera del CDE. Las entidades deben considerar si los factores que contribuyeron a generar la situación, como los procesos de negocios, el comportamiento del usuario, las configuraciones incorrectas del sistema, etc., causaron que los datos PAN se almacenaran en una ubicación inesperada. Si tales factores están presentes, deben abordarse según este Requisito para evitar que la situación se repita.
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** El uso de mecanismos para detectar y prevenir la salida de datos PAN no autorizados del CDE, permite a la organización detectar e impedir situaciones que pueden conducir a la pérdida de datos. **Buenas Prácticas** La cobertura de los mecanismos debe incluir, entre otros, correos electrónicos, descargas a medios extraíbles y salidas a impresoras. **Ejemplos** Los mecanismos para detectar y prevenir la pérdida no autorizada de datos PAN no cifrados pueden incluir el uso de herramientas adecuadas, como soluciones de prevención de pérdida de datos (DLP), así como procesos y procedimientos manuales.
A3.2.6 Se implementan mecanismos para detectar e impedir que los datos PAN no cifrados abandonen el CDE a través de un canal, método o proceso no autorizado, incluidos mecanismos como: • Ejecución permanente. • Configurar para detectar y evitar que los datos PAN no cifrados abandonen el CDE a través de un canal, método o proceso no autorizado. • Generar registros de auditoría y alertas al detectar datos PAN no cifrados que salen del CDE a través de un canal, método o proceso no autorizado. **Términos de Referencia PCI DSS**: *Alcance de los Requisitos de PCI DSS, Requisito 12*	**A3.2.6.a** Evalúe la documentación y estudiar los mecanismos implementados para verificar que cumplan con todos los elementos especificados en este requisito. **A3.2.6.b** Evalúe los registros de auditoría y las alertas, y entreviste al personal responsable para verificar que se investiguen las alertas.	

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Este requisito no es apto para el enfoque personalizado.		
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Los intentos de eliminar datos PAN no cifrados a través de un canal, método o proceso no autorizado pueden indicar un intento malicioso de robar datos, o pueden ser generados por acciones de un empleado autorizado que desconoce o simplemente no sigue los métodos adecuados. La investigación rápida de estos sucesos puede identificar dónde se deben aplicar las correcciones y proporciona información valiosa para ayudar a comprender de dónde provienen las amenazas.
A3.2.6.1 Los procedimientos de respuesta se implementan para ser iniciados ante la detección de intentos de eliminar datos PAN no cifrados del CDE a través de un canal, método o proceso no autorizado. Los procedimientos de respuesta incluyen: • Procedimientos para la pronta investigación de alertas por parte del personal responsable. • Procedimientos para remediar fugas de datos o brechas del proceso, según sea necesario, para evitar cualquier pérdida de datos. **Términos de Referencia PCI DSS**: *Requisito 12*	**A3.2.6.1.a** Evalúe los procedimientos de respuesta documentados para verificar que los procedimientos para responder a un intento de eliminar datos PAN no cifrados del CDE a través de un canal, método o proceso no autorizado incluyen todos los elementos especificados en este requisito: • Procedimientos para la pronta investigación de alertas por parte del personal responsable. • Procedimientos para remediar fugas de datos o brechas del proceso, según sea necesario, para evitar cualquier pérdida de datos.	
Objetivo del Enfoque Personalizado Este requisito no es apto para el enfoque personalizado.	**A3.2.6.1.b** Entreviste al personal y Evalúe los registros de las acciones tomadas cuando se detectan datos PAN no cifrados saliendo del CDE a través de un canal, método o proceso no autorizado y verifique que se hayan realizado actividades correctivas.	

Requisitos y Procedimientos de Prueba		Guía
A3.3 PCI DSS se incorpora a las actividades habituales (BAU).		
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	
A3.3.1 Las fallas de los sistemas críticos de control de seguridad se detectan, alertan y son abordados de inmediato, incluyendo, entre otros, las fallas de: • Controles de seguridad de la red • IDS/IPS • FIM • Soluciones antimalware: • Controles de acceso físico • Controles de acceso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan) • Mecanismos de revisión automatizados del registro de auditoría. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; consulte las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.* • Herramientas de revisión de código automatizadas (si se utilizan). *Este punto es una de las mejores prácticas hasta su fecha de vigencia; consulte las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.* **Términos de Referencia PCI DSS**: *Requisitos 1-12* *(continúa en la página siguiente)*	**A3.3.1.a** Evalúe las políticas y los procedimientos documentados para verificar estén definidos para detectar, alertar y abordar rápidamente las fallas críticas de control de seguridad de acuerdo con todos los elementos especificados en este requisito. **A3.3.1.b** Evalúe los procesos de detección y alerta, y entreviste al personal para verificar que se implementen procesos para todos los controles de seguridad críticos especificados en este requisito y que cada falla de un control de seguridad crítico genere una alerta.	**Propósito** Sin procesos formales para la pronta (tan pronto como sea posible) detección, alerta y tratamiento de fallas críticas de control de seguridad, las fallas pueden pasar desapercibidas o permanecer sin resolver durante períodos prolongados. Además, sin procesos formales con límite de tiempo, los atacantes tendrán tiempo suficiente para comprometer los sistemas y robar datos de cuentas del CDE. **Buenas Prácticas** Los tipos específicos de fallas pueden variar dependiendo de la función del componente del sistema del dispositivo y la tecnología en uso. Las fallas típicas incluyen que el sistema cese de realizar sus funciones de seguridad o que no funcione de la manera prevista, como un *firewall* que borra todas sus reglas o se desconecta.

Requisitos y Procedimientos de Prueba		Guía
Objetivo del Enfoque Personalizado Este requisito no es apto para el enfoque personalizado.		
Notas de Aplicabilidad *Los puntos anteriores (para los mecanismos de revisión de registros automatizados y las herramientas de revisión de código automatizadas (si se usan)) son mejores prácticas hasta el 31 de marzo de 2025, después de lo cual se requerirán como parte del Requisito A3.3.1 y deben tomarse en cuenta en su totalidad durante una evaluación PCI DSS.*		

Requisitos y Procedimientos de Prueba		Guía
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Si las alertas de fallas de los sistemas de control de seguridad críticos no se responden de manera rápida y efectiva, los atacantes pueden usar este tiempo para insertar software malicioso, obtener el control de un sistema o robar datos del entorno de la entidad. **Buenas Prácticas** La evidencia documentada (por ejemplo, los registros dentro de un sistema de gestión de problemas) debe respaldar los procesos y procedimientos existentes que respondan a las fallas de seguridad. Además, el personal debe conocer sus responsabilidades en caso de fallas. Las acciones y respuestas a las fallas deben capturarse en la evidencia documentada.
A3.3.1.2 Las fallas en los sistemas de control de seguridad críticos se atienden con prontitud. Los procesos para responder a las fallas en los sistemas de control de seguridad incluyen: • Restaurando las funciones de seguridad. • Identificando y documentando la duración (fecha y hora de principio a fin) de la falla de seguridad. • Identificar y documentar las causas de la falla, incluyendo la raíz del problema, y documentar la corrección requerida para abordar la raíz del problema. • Identificando y abordando cualquier problema de seguridad que surgió durante la falla. • Determinar si se requieren más acciones como resultado de la falla de seguridad. • Implementar controles para evitar que se repita la causa de la falla. • Reanudación del monitoreo de los controles de seguridad. **Términos de Referencia PCI DSS**: *Requisitos 1-12*	**A3.3.1.2.a** Evalúe las políticas y los procedimientos documentados y entreviste al personal para verificar que los procesos estén definidos e implementados a fin de responder rápidamente a una falla en el control de seguridad de acuerdo con todos los elementos especificados en este requisito. **A3.3.1.2.b** Evalúe los registros para verificar que las fallas en los controles de seguridad estén documentadas e incluyan: • Identificación de las causas de la falla, incluida la raíz del problema. • Duración (fecha y hora de inicio y finalización) del fallo de seguridad. • Detalles de la rehabilitación necesaria para abordar raíz del problema.	
Objetivo del Enfoque Personalizado		
Este requisito no es apto para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito** Las tecnologías de hardware y software están en constante evolución, y las organizaciones deben estar al tanto de los cambios en las tecnologías que se utilizan, así como de las amenazas en evolución para esas tecnologías. La realización de revisiones adecuadas de estas tecnologías garantiza que la organización pueda prepararse y gestionar las vulnerabilidades en el hardware y el software que el proveedor o el desarrollador no corregirán. **Buenas Prácticas** Las organizaciones también deben considerar revisar las versiones de firmware para asegurarse de que permanezcan actualizadas y respaldadas por los proveedores. Las organizaciones también deben conocer los cambios realizados por los proveedores de tecnología en sus productos o procesos a fin de comprender cómo dichos cambios pueden afectar el uso de cada tecnología por parte de la organización. Las revisiones periódicas de las tecnologías que impactan o influyen en los controles PCI DSS pueden ayudar con las estrategias de compra, uso e implementación, y garantizar que los controles que dependen de esas tecnologías sigan siendo eficientes. Estas revisiones incluyen, entre otras, la revisión de tecnologías que ya no son compatibles con el proveedor y/o que ya no satisfacen las necesidades de seguridad de la organización.
A3.3.2 Las tecnologías de hardware y software se revisan al menos una vez cada 12 meses para confirmar si continúan cumpliendo con los requisitos de PCI DSS de la organización. **Términos de Referencia PCI DSS**: *Requisitos 2, 6, 12.*	**A3.3.2.a** Evalúe las políticas y los procedimientos documentados y entreviste al personal para verificar que los procesos estén definidos e implementados para revisar las tecnologías de hardware y software a fin de confirmar si continúan cumpliendo con los requisitos de PCI DSS de la organización.	
	A3.3.2.b Revise los resultados de las revisiones recientes de tecnologías de hardware y software para verificar que las revisiones se realicen al menos una vez cada 12 meses.	
Objetivo del Enfoque Personalizado Este requisito no es apto para el enfoque personalizado.	**A3.3.2.c** Revise la documentación para verificar que, para cualquier tecnología que se haya determinado que ya no cumple con los requisitos de PCI DSS de la organización, existe un plan para corregir esa tecnología.	
Notas de Aplicabilidad El proceso incluye un plan para corregir tecnologías que ya no cumplen con los requisitos de PCI DSS de la organización, hasta e incluyendo el reemplazo de la tecnología, según corresponda.		

Requisitos y Procedimientos de Prueba		Guía
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	
A3.3.3 Las revisiones se realizan al menos una vez cada tres meses para verificar que se cumple con las actividades BAU. Las revisiones son realizadas por personal asignado al programa de cumplimiento PCI DSS (como se identifica en A3.1.3), e incluyen: • Confirmación de que se están realizando todas las actividades BAU, incluidas A3.2.2, A3.2.6 y A3.3.1. • Confirmación de que el personal cumple con las políticas de seguridad y los procedimientos operativos (por ejemplo, revisiones de registros diarios, revisiones de conjuntos de reglas para controles de seguridad de red, estándares de configuración para nuevos sistemas). • Documentar cómo se completaron las revisiones, incluida la forma en que se verificó que todas las actividades BAU estaban en su lugar. • Recopilación de evidencia documentada según lo requerido para la evaluación anual PCI DSS. • Revisión y aprobación de los resultados por parte del personal responsable del programa de cumplimiento PCI DSS, como se identifica en A3.1.3. • Conservación de registros y documentos por al menos 12 meses, cubriendo todas las actividades BAU. **Términos de Referencia PCI DSS**: *Requisitos 1-12*	**A3.3.3.a** Evalúe las políticas y los procedimientos para verificar que los procesos estén definidos para revisar y verificar las actividades BAU de acuerdo con todos los elementos especificados en este requisito. **A3.3.3.b** Entreviste al personal responsable y Evalúelos registros de revisiones para verificar que: • Las revisiones son realizadas por personal asignado al programa de cumplimiento PCI DSS. • Las revisiones se realizan al menos una vez cada tres meses.	**Propósito** La confirmación periódica de que se están siguiendo las políticas y los procedimientos de seguridad garantiza que los controles esperados estén activos y funcionando según lo previsto. El objetivo de estas revisiones no es volver a desempeñar con otros requisitos de PCI DSS, sino confirmar que las actividades de seguridad se realizan de manera continua. **Buenas Prácticas** Estas revisiones también se pueden usar para verificar que se mantenga la evidencia adecuada, por ejemplo, registros de auditoría, informes de exploración de vulnerabilidades, revisiones de conjuntos de reglas de control de seguridad de la red, para ayudar en la preparación de la entidad para su próxima evaluación PCI DSS. **Ejemplos** Tomando como ejemplo el Requisito 1.2.7, el Requisito A3.3.3 se cumple al confirmar, al menos una vez cada tres meses, que las revisiones de las configuraciones de los controles de seguridad de la red se han realizado con la frecuencia requerida. Por otro lado, el Requisito 1.2.7 se cumple al revisar esas configuraciones como se especifica en el requisito.
Objetivo del Enfoque Personalizado		
Este requisito no es apto para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
A3.4 Se controla y gestiona el acceso lógico al entorno de datos del titular de la tarjeta.		
Requisitos de Enfoques Definidos	**Procedimientos de Prueba del Enfoque Definido**	**Propósito**
A3.4.1 Las cuentas de usuario y los privilegios de acceso a los componentes del sistema dentro del alcance, se revisan al menos una vez cada seis meses para garantizar que las cuentas de usuario y los privilegios de acceso sigan siendo apropiados según la posición de trabajo, y que todo acceso está autorizado. **Términos de Referencia PCI DSS**: *Requisito 7*	**A3.4.1** Entreviste al personal responsable y Evalúe la documentación de apoyo para verificar que: • Las cuentas de usuario y los privilegios de acceso se revisan al menos cada seis meses. • Las revisiones confirman que el acceso es apropiado según el puesto de trabajo y que todo acceso está autorizado.	La revisión periódica de los derechos de acceso ayuda a detectar los derechos de acceso excesivos que quedan después de que cambian las responsabilidades laborales de los usuarios, las funciones del sistema u otras modificaciones. Si los derechos de usuario excesivos no se revocan a su debido tiempo, pueden ser utilizados por usuarios malintencionados para acceder sin autorización. Esta revisión ofrece otra oportunidad para garantizar que se han eliminado las cuentas de todos los usuarios dados de baja (si es que faltaba alguna en el momento de la baja), así como también para asegurarse de que se haya dado de baja a cualquier tercero que ya no necesite acceso.
Objetivo del Enfoque Personalizado		
Este requisito no es apto para el enfoque personalizado.		

Requisitos y Procedimientos de Prueba		Guía
A3.5 Los eventos sospechosos son identificados y respondidos.		
Requisitos de Enfoques Definidos **A3.5.1** Se implementa una metodología para identificar rápidamente patrones de ataque y comportamientos no deseados en todos los sistemas que incluye: • Identificación de anomalías o actividades sospechosas a medida que se producen. • Emisión de alertas rápidas dirigidas personal responsable, al detectar actividades sospechosas o anomalías. • Respuesta a alertas de acuerdo con los procedimientos de respuesta documentados. **Términos de Referencia PCI DSS**: *Requisitos 10, 12* **Objetivo del Enfoque Personalizado** Este requisito no es apto para el enfoque personalizado.	**Procedimientos de Prueba del Enfoque Definido** **A3.5.1.a** Evalúe la documentación y entreviste al personal para verificar que se haya definido e implementado rápidamente una metodología para identificar patrones de ataque y comportamientos no deseados en los sistemas, que incluya todos los elementos especificados en este requisito. **A3.5.1.b** Evalúe los procedimientos de respuesta a incidentes y entreviste al personal responsable para verificar que: • El personal de guardia recibe alertas rápidas. • Se responde a las alertas siguiendo los procedimientos de respuesta documentados.	**Propósito** La capacidad de identificar patrones de ataque y comportamientos indeseables en todos los sistemas, por ejemplo, utilizando herramientas de correlación de registros automatizadas o administradas centralmente, es fundamental para impedir, detectar o minimizar el impacto de datos comprometidos. La presencia de registros en todos los entornos permite el seguimiento, alerta y análisis exhaustivos cuando algo sale mal. Sin un proceso para corroborar la información de los componentes críticos del sistema y los sistemas que realizan funciones de seguridad, como controles de seguridad de red, IDS/IPS y sistemas de monitoreo de integridad de archivos (FIM), determinar las causas de una situación comprometida, es muy difícil o casi imposible. Por lo tanto, los registros de todos los componentes críticos del sistema y los sistemas que realizan funciones de seguridad deben recopilarse, correlacionarse y mantenerse. Esto podría incluir el uso de productos de software y metodologías de servicio para proporcionar análisis, alertas e informes en tiempo real, tales como información de seguridad y gestión de eventos (SIEM), FIM o detección de cambios.

Anexo B Controles Compensatorios

Los controles compensatorios pueden considerarse cuando una entidad no puede cumplir un requisito de PCI DSS tal y como está indicado, debido a limitaciones técnicas o empresariales legítimas documentadas, pero ha mitigado suficientemente el riesgo asociado al requisito mediante la aplicación de otros controles, o controles compensatorios.

Los controles compensatorios deben satisfacer los siguientes criterios:

1. Cumplir con la intención y el rigor del requisito original PCI DSS.
2. Proporcionar un nivel de defensa similar al del requisito original PCI DSS, de manera que el control compensatorio neutralice suficientemente el riesgo contra el que se diseñó el requisito original PCI DSS. Para entender la intención de un requisito, refiérase a *Objetivo del Enfoque Personalizado* para la mayoría de los requisitos de PCI DSS. Si un requisito no es elegible para el Enfoque Personalizado y, por lo tanto, no tiene un Objetivo del Enfoque Personalizado, consulte el **Propósito** en la columna de Orientación para ese requisito.
3. Ir "más allá" de otros requisitos de PCI DSS. (El simple hecho de cumplir con otros requisitos de PCI DSS no es un control compensatorio).
4. Al evaluar "por encima y más allá" los controles compensatorios, tenga en cuenta lo siguiente:

   Nota: *Todos los controles compensatorios deben ser revisados y validados en cuanto a su suficiencia por el asesor que realiza la evaluación PCI DSS. La eficiencia de un control compensatorio depende de las características específicas del entorno en el que se implementa el control, los controles de seguridad circundantes y la configuración del control. Las entidades deben ser conscientes de que un determinado control compensatorio no será eficiente en todos los entornos.*

   a. Los requisitos existentes PCI DSS NO PUEDEN considerarse controles compensatorios si ya se exigen para el elemento que se está revisando. Por ejemplo, las contraseñas para el acceso administrativo sin consola deben enviarse cifradas para mitigar el riesgo de interceptar las contraseñas administrativas no cifradas. La entidad no puede utilizar otros requisitos de contraseñas PCI DSS (bloqueo de intrusos, contraseñas complejas, etc.) para compensar la falta de contraseñas cifradas, ya que esos otros requisitos de contraseñas no mitigan el riesgo de interceptación de contraseñas no cifradas. Además, los otros controles de contraseñas ya son requisitos de PCI DSS para el elemento en revisión (contraseñas).
   b. Los requisitos de PCI DSS existentes PUEDEN ser considerados como controles compensatorios si son requeridos para otra área, pero no son requeridos para el ítem bajo revisión.

c. Los requisitos de PCI DSS existentes pueden combinarse con nuevos controles para convertirse en un control compensatorio. Por ejemplo, si una empresa no tiene la capacidad de abordar una vulnerabilidad explotable a través de una interfaz de red porque la actualización de seguridad no está disponible por parte de un proveedor, un control compensatorio podría consistir en controles que incluyan todo lo siguiente: 1) segmentación interna de la red, 2) limitar el acceso a la red para la interfaz vulnerable sólo a los dispositivos necesarios (filtrado de direcciones IP o MAC), y 3) monitoreo IDS/IPS de todo el tráfico destinado a la interfaz vulnerable.

5. Abordar el riesgo adicional que supone no cumplir con el requisito de PCI DSS.
6. Abordar el requisito en la actualidad y en el futuro. Un control compensatorio no puede abordar un requisito que no se cumplió en el pasado (por ejemplo, cuando se exigió la realización de una tarea hace dos trimestres, pero esa tarea no se realizó).

El asesor debe evaluar a fondo los controles compensatorios durante cada evaluación anual PCI DSS para confirmar que cada control compensatorio aborda adecuadamente el riesgo para el que se diseñó el requisito original PCI DSS, según los puntos 1 a 5 anteriores.

Para mantener el cumplimiento, deben existir procesos y controles que garanticen que los controles compensatorios sigan siendo eficientes una vez finalizada la evaluación. Además, los resultados de los controles compensatorios deben documentarse en el informe aplicable para la evaluación (por ejemplo, un Informe de Cumplimiento o un Cuestionario de Autoevaluación) en la sección correspondiente del requisito de PCI DSS, e incluirse cuando el informe aplicable se presente a la organización solicitante.

Anexo C Ficha de Control Compensatorio

La entidad debe utilizar esta ficha para definir los controles compensatorios para cualquier requisito en el que se utilicen controles compensatorios para cumplir un requisito de PCI DSS. Tenga en cuenta que los controles compensatorios también deben documentarse de acuerdo con las instrucciones del Informe de Cumplimiento en la sección correspondiente PCI DSS.

Nota: *Sólo las entidades que tengan limitaciones tecnológicas o empresariales legítimas y documentadas pueden considerar el uso de controles compensatorios para lograr el cumplimiento.*

Número de Requisito y Definición:

	Información Requerida	Explicación
1. Restricciones	Documente las limitaciones técnicas o empresariales legítimas que impiden el cumplimiento del requisito original.	
2. Definición de los Controles Compensatorios	Defina los controles compensatorios: explique cómo abordan los objetivos del control original y el aumento del riesgo si lo hay.	
3. Objetivo	Defina el objetivo del control original (por ejemplo, el Objetivo del Enfoque Personalizado).	
	Identifique el objetivo que cumple el control compensatorio *(nota: puede ser, pero no es obligatorio, el Objetivo del Enfoque Personalizado establecido para el requisito de PCI DSS).*	
4. Riesgo Identificado	Identifique cualquier riesgo adicional que suponga la falta del control original.	
5. Validación de los Controles compensatorios	Defina cómo se validaron y comprobaron los controles compensatorios.	
6. Mantenimiento	Defina los procesos y controles establecidos para mantener los controles compensatorios.	

Anexo D Enfoque Personalizado

Este enfoque está destinado a las entidades que deciden cumplir con los requisitos de PCI DSS con el Objetivo del Enfoque Personalizado de manera que no sigue estrictamente el requisito definido. El enfoque personalizado permite a una entidad adoptar un enfoque estratégico para cumplir el Objetivo del Enfoque Personalizado de un requisito, de modo que puede determinar y diseñar los controles de seguridad necesarios para cumplir con ese objetivo de forma única para esa organización.

La entidad que implemente un enfoque personalizado debe cumplir con los siguientes criterios:

- Documentar y mantener evidencias sobre cada control personalizado, incluyendo toda la información especificada en la Plantilla de Matriz de Controles del Anexo E1.
- Realizar y documentar un análisis de riesgos específicos (requisito 12.3.2 PCI DSS) para cada control personalizado, incluyendo toda la información especificada en la Plantilla de Análisis de Riesgo Específicos del Anexo E2.
- Realice pruebas de cada control personalizado para demostrar su eficiencia y documente las pruebas realizadas, los métodos utilizados, lo que se evaluó, cuándo se realizaron las pruebas y los resultados de las mismas en la matriz de controles.
- Monitorear y mantener evidencia de las pruebas sobre la eficiencia de cada control personalizado.
- Proporcionar a su asesor las matrices completas de los controles desarrolladas, el análisis de riesgos específico, las pruebas y las pruebas de la eficiencia del control personalizado.

El asesor que desarrolle una evaluación de los controles personalizados debe cumplir los siguientes criterios:

- Revisar las matrices de controles de la entidad, el análisis de riesgos específicos y las evidencias de eficiencia del control para comprender plenamente los controles personalizados y verificar que la entidad cumple con todos los requisitos de documentación y evidencias del Enfoque Personalizado.
- Derivar y documentar los procedimientos de prueba apropiados necesarios para desarrollar pruebas exhaustivas de cada control personalizado.
- Probar cada control personalizado para determinar si la implementación de la entidad 1) cumple con el Objetivo del Enfoque Personalizado del requisito y 2) da lugar a un resultado "en cumplimiento" para el requisito.
- En todo momento, los QSA mantienen los requisitos de independencia definidos en los Requerimientos de Calificación como QSA. Esto significa que, si un QSA participa en el diseño o la implantación de un control personalizado, dicho QSA no debería definir también los procedimientos de prueba, ni evaluar, ni colaborar en la evaluación de dicho control personalizado.

Se espera que la entidad y su asesor trabajen juntos para asegurarse que 1) están de acuerdo en que el control o los controles personalizados cumplen plenamente el Objetivo del Enfoque Personalizado, 2) el asesor comprende plenamente el control personalizado y 3) la entidad comprende las pruebas derivadas que realizará el asesor.

El uso del enfoque personalizado debe ser completado por un QSA o ISA y debe ser documentado de acuerdo con las instrucciones de la Plantilla de Informe de Cumplimiento (ROC) y siguiendo las instrucciones del FAQs *para el uso de la Plantilla del ROC PCI DSS v4.0* disponibles en el sitio web PCI SCC.

Las entidades que completan un Cuestionario de Autoevaluación (SAQ) no son elegibles para aplicar un enfoque personalizado; sin embargo, estas entidades pueden elegir que un QSA o ISA realicen su evaluación y la documente en una Plantilla ROC.

El uso del enfoque personalizado puede estar regulado por organizaciones que gestionan programas de cumplimiento (por ejemplo, marcas de pago y adquirentes). Por lo tanto, las preguntas acerca del uso de un enfoque personalizado deben remitirse a esas organizaciones, incluyendo, por ejemplo, si una entidad requiere utilizar un QSA, o si puede utilizar un ISA para completar una evaluación utilizando el enfoque personalizado.

Nota: *Los controles compensatorios no son una opción con el enfoque personalizado. Debido a que el enfoque personalizado permite a una entidad determinar y diseñar los controles necesarios para cumplir con el Objetivo del Enfoque Personalizado de un requisito, se espera que la entidad implemente efectivamente los controles que diseñó para ese requisito sin necesidad de implementar también controles alternativos y compensatorios.*

Anexo E Ejemplos de Plantillas para Respaldar el Enfoque Personalizado

Este anexo contiene ejemplos de plantillas para la matriz de controles y el análisis de riesgos específicos que la entidad debe documentar como parte del enfoque personalizado. Estas plantillas constituyen ejemplos de formatos que podrían utilizarse. *Aunque no es obligatorio que las entidades sigan los formatos específicos proporcionados en este anexo, la matriz de control y el análisis de riesgos específicos de la entidad deben incluir toda la información definida en estas plantillas.*

E1 Ejemplo de Plantilla de Matriz de Control

El siguiente es un ejemplo de la plantilla de matriz de control que puede ser utilizado por una entidad para documentar su implementación personalizada.

Como se describe en el *Anexo D: Enfoque Personalizado,* las entidades que utilizan el enfoque personalizado deben completar una matriz de control para proporcionar detalles de cada control implementado que explique qué se implementa, cómo ha determinado la entidad que los controles cumplen con el objetivo declarado de un requisito de PCI DSS, cómo el control proporciona al menos, el nivel de protección equivalente al que se lograría al cumplir con el requisito definido, y cómo la entidad tiene la seguridad sobre la eficiencia del control de forma continua.

El asesor utiliza la información dentro de cada matriz de control para planificar y prepararse para la evaluación.

Este ejemplo de plantilla de matriz de control incluye la información mínima que debe documentar la entidad y proporcionar al asesor para una validación personalizada. Si bien no se requiere el uso de esta plantilla específica, se requiere que la documentación del enfoque personalizado de la entidad incluya toda la información definida en esta plantilla, y que la entidad proporcione esta información exacta a su asesor.

La matriz de control no reemplaza la necesidad de que el asesor desarrolle de forma independiente procedimientos de prueba apropiados para validar los controles implementados. El asesor aún debe realizar las pruebas necesarias para verificar que los controles cumplan con el objetivo del requisito, sean eficientes y se mantengan de forma apropiada. La matriz de control tampoco reemplaza los requisitos de informes para validaciones personalizadas como se especifica en la plantilla ROC.

La matriz de control deberá incluir al menos la información de la siguiente tabla.

Ejemplo de Plantilla de Matriz de Control para los requisitos de PCI DSS cubiertos a través del Enfoque Personalizado **Para ser completado por la entidad evaluada**		
Identificador/Nombre de Control Personalizado	<La entidad define cómo quiere referirse a este control>	
Número de requisitos de PCI DSS y objetivos que se cumplen con este control.	Requisito #: Requisito #:	Objetivo: Objetivo:
Detalles del control		
¿Cuáles son los controles implementados?	<La entidad describe qué es el control y qué hace>	
¿Dónde se implementan los controles?	<La entidad identifica las ubicaciones de las instalaciones y los componentes del sistema donde se implementa y gestiona el control>	
¿Cuándo se realizan los controles?	<La entidad detalla con qué frecuencia se realiza el control; por ejemplo, se ejecuta continuamente en tiempo real o está programado para ejecutarse en NN horas y en XX intervalos>	
¿Quién tiene la responsabilidad general y la rendición de cuentas de los controles?	<La entidad incluye detalles del personal/funciones individuales con responsabilidad y rendición de cuentas para este control>	
¿Quién participa en la gestión, el mantenimiento y el monitoreo de los controles?	<La entidad incluye detalles del personal individual/funciones y/o equipos, según corresponda, que gestionan, mantienen y monitorean el control>	
***Para cada* requisito de PCI DSS para el cual se utilicen los controles, la entidad proporciona detalles de lo siguiente:**		
La entidad describe cómo los controles implementados cumplen con el ***Objetivo del Enfoque Personalizado*** establecido del requisito de PCI DSS.	<La entidad describe cómo el control cumple con el Objetivo del Enfoque Personalizado establecido del requisito de PCI DSS y resume los resultados relacionados>	

Ejemplo de Plantilla de Matriz de Control para los requisitos de PCI DSS cubiertos a través del Enfoque Personalizado Para ser completado por la entidad evaluada	
La entidad describe las pruebas **que realizó** y los resultados de esas pruebas que demuestran que los controles cumplen con el objetivo del requisito aplicable.	<La entidad describe las pruebas que realizó para demostrar que el control cumple con el objetivo declarado del requisito de PCI DSS y resume los resultados relacionados>
La entidad describe brevemente los resultados del análisis de riesgo específico individual **que realizó** que explica los controles implementados y describe cómo los resultados verifican que los controles brindan al menos un nivel de protección equivalente al del enfoque definido por el requisito de PCI DSS aplicable. *Consulte la Plantilla de Análisis de Riesgos Específicos para obtener detalles sobre cómo documentar este análisis de riesgos*.	<La entidad describe brevemente los resultados de su análisis de riesgo para este control, el cual se detalla por separado en el Análisis de Riesgo Específico>
La entidad describe las medidas **que ha implementado** para garantizar que se mantengan los controles y se garantice su eficiencia de forma continua. *Por ejemplo, cómo la entidad supervisa la eficiencia en el control, cómo se detectan y responden las fallas de control, y las acciones que se toman.*	<La entidad describe cómo asegura que se mantenga el control y cómo se asegura la eficiencia del control.>

E2 Ejemplo de Plantilla de Análisis de Riesgo Específico

La siguiente es una muestra de una plantilla de análisis de riesgo específico que la entidad puede usar para su implementación personalizada. *Si bien no se requiere que la entidad siga este formato específico, la documentación de su enfoque personalizado debe incluir toda la información definida en esta plantilla.*

Como se describe en el *Anexo D: Enfoque Personalizado y, de acuerdo con el requisito 12.3.2 PCI DSS, una entidad que utilice el enfoque personalizado debe proporcionar un análisis de riesgo específico detallado para cada requisito que la entidad cumpla con el enfoque personalizado.* El análisis de riesgo define el riesgo, evalúa el efecto sobre la seguridad si no se cumple el requisito definido y describe cómo la entidad ha determinado que los controles brindan al menos un nivel de protección equivalente al proporcionado por el requisito de PCI DSS definido.

El asesor utiliza la información en el análisis de riesgo específico para planificar y prepararse para la evaluación.

Al completar un análisis de riesgo específico para un enfoque personalizado, es importante recordar que:

- El activo que se protege son los datos de titulares de tarjetas que la entidad almacena, procesa o transmite.
- Los agentes amenazas están altamente motivados y capaces. La motivación y la capacidad de los agentes de amenazas tiende a aumentar en relación con el volumen de datos de titulares de tarjetas que generará un ataque exitoso.
- La probabilidad de que una entidad sea atacada por agentes de amenazas aumenta a medida que la entidad almacena, procesa o transmite mayores volúmenes de datos de titulares de tarjetas.
- El daño está directamente relacionado con el objetivo. Por ejemplo, si el objetivo es "el software malicioso no puede ejecutarse", el daño es que el software malicioso se ejecute; si el objetivo es "se asignan responsabilidades diarias para realizar todas las actividades", el daño es que no se asignan las responsabilidades.

***Nota**: El término "daño" tal como se usa en este análisis de riesgo específico (por ejemplo, en 1.3 en la tabla a continuación) se refiere a una ocurrencia o evento que afecta negativamente la postura de seguridad de la entidad. Ejemplos de esto lo constituyen la ausencia de una política, la falla en realizar un escaneo de vulnerabilidades o que se ejecute malware en el entorno de la entidad.*

Esta muestra de plantilla de análisis de riesgo específico incluye la información mínima que debe documentar la entidad y proporcionar al asesor para una validación personalizada. Si bien no se requiere el uso de esta plantilla específica, se requiere que la documentación del enfoque personalizado de la entidad incluya toda la información definida en esta plantilla, y que la entidad proporcione esta información exacta a su asesor.

El análisis de riesgos específico debe incluir al menos la información de la siguiente tabla.

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada	
Ítem	**Detalles**
1. Identificar el requisito	
1.1 Identifique el requisito de PCI DSS tal como está escrito.	<La entidad identifica el requisito>
1.2 Identifique el objetivo del requisito de PCI DSS tal como está escrito.	<La entidad identifica el objetivo del requisito>

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada	
Ítem	**Detalles**
1.3 Describa el daño que el requisito pretendía impedir.	<La entidad describe el daño> <La entidad describe el efecto sobre su seguridad si la entidad no cumple con éxito el objetivo.> <La entidad describe qué fundamentos de seguridad cumplen, o qué podría hacer un agente de amenazas si la entidad no cumple con éxito el objetivo.>
2. Describa la solución propuesta	
2.1 Identificador/Nombre de Control Personalizado	<La entidad identifica el control personalizado como se documenta en la Matriz de Controles.>
2.2 ¿Qué partes del requisito tal como está escrito cambiarán en la solución propuesta?	<La entidad identifica qué elementos del requisito no se cumplirán con el enfoque definido y, por lo tanto, estarán cubiertos por el enfoque personalizado. Esto podría ser tan pequeño como cambiar la periodicidad de un requisito o la implementación de un conjunto de controles completamente diferente para cumplir el objetivo.>
2.3 ¿Cómo evitará el daño la solución propuesta?	<La entidad describe cómo los controles detallados en la Matriz de Controles evitarán los daños identificados en 1.3.>

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada						
Ítem	**Detalles**					
3. Analice cualquier cambio en la PROBABILIDAD de que ocurra el daño, lo que lleva a una brecha de la confidencialidad de los datos de titulares de tarjetas.						
3.1 Describa los factores detallados en la Matriz de Control que afectan la probabilidad de que ocurra el daño.	La entidad describe: • Qué tan exitosos serán los controles para prevenir el daño • Cómo los controles detallados en la Matriz de Control reducen la probabilidad de que ocurra el daño					
3.2 Describa las razones por las que el daño puede seguir ocurriendo después de la aplicación del control personalizado.	La entidad describe: • Las razones típicas por las que falla el control, la probabilidad de que esto ocurra y cómo podría evitarse • ¿Qué tan resilientes son los procesos y sistemas de la entidad para detectar que los controles no están operando normalmente? • ¿Cómo un agente de amenazas podría eludir este control? - ¿Qué pasos deberían tomar? ¿qué tan difícil es, se detectaría al agente de amenazas antes de que fallara el control? ¿Cómo se ha determinado esto?					
3.3 ¿En qué medida los controles detallados en el enfoque personalizado representan un cambio en la probabilidad de ocurrencia del daño en comparación con el requisito de enfoque definido?	El daño es más susceptible de ocurrir	☐	No hay cambios	☐	El daño es menos susceptible de ocurrir	☐
3.4 Proporcione el razonamiento de su evaluación del cambio en la probabilidad de que ocurra el daño una vez que se implementen los controles personalizados.	La entidad provee: • La justificación de la evaluación documentada en 3.3. • Los criterios y valores utilizados para la evaluación documentada en 3.3.					

Ejemplo de Análisis de Riesgo Específico para los requisitos de PCI DSS cumplidos a través del Enfoque Personalizado. Para ser completado por la entidad evaluada				
Ítem	**Detalles**			
4. Analice cualquier cambio en el IMPACTO del acceso no autorizado a los datos de la cuenta				
4.1 Para el alcance de los componentes del sistema que cubre esta solución, ¿qué volumen de datos de cuentas estaría en riesgo de acceso no autorizado si la solución fallara?	**4.1.1** Número de datos PAN almacenados	*Máximo en cualquier momento*	**4.1.2** Número de datos PAN procesados o transmitidos durante un período de 12 meses	*Total*
4.2 Descripción de cómo los controles personalizados serán direccionados: • Reducirán la cantidad de datos PAN individuales comprometidos si un agente de amenazas tiene éxito, y/o • Permitirán una notificación más rápida de los datos PAN comprometidos con las marcas de tarjetas.	El impacto en el ecosistema de pago está directamente relacionado con la cantidad de cuentas comprometidas y con qué rapidez el emisor de la tarjeta puede bloquear cualquier dato PAN que haya quedado comprometido. La entidad describe cómo los controles personalizados logran lo siguiente, para cada uno de los controles personalizados: • Reduce el volumen de datos de titulares de tarjetas que se almacenan, procesan o transmiten y, por lo tanto, reduce los elementos disponibles para que un agente de amenazas tenga éxito, y/o • Reduce el tiempo de detección, notificación de cuentas comprometidas y contención del agente de amenazas.			
5. Aprobación y revisión de riesgos				
5.1 He revisado el análisis de riesgos anterior y acepto que el uso del enfoque personalizado propuesto como se detalla proporciona al menos un nivel de protección equivalente al enfoque definido para el requisito de PCI DSS aplicable.	Un miembro de la dirección ejecutiva debe revisar y aceptar el enfoque personalizado propuesto. <Un miembro de la gerencia ejecutiva de la entidad firma que revisó y aceptó el enfoque personalizado documentado aquí.>			
5.2 Este análisis de riesgos debe revisarse y actualizarse a más tardar:	El análisis de riesgos debe revisarse al menos cada doce meses, y con mayor frecuencia si el enfoque personalizado en sí tiene un límite de tiempo (por ejemplo, porque hay un cambio planificado en la tecnología) o si otros factores dictan un cambio necesario. En caso de una revisión de riesgo no programada, detalle el motivo por el cual se realizó la revisión. <La entidad indica la fecha en que se revisó y actualizó el análisis de riesgo específico.>			

Anexo F Aprovechamiento del Marco de Seguridad del Software PCI para Cumplir con el Requisito 6

El Requisito 6 PCI DSS define los requisitos para el desarrollo y mantenimiento de sistemas y software seguros. Debido a que el Estándar de Software Seguro y el Estándar SLC Seguro (colectivamente, el Marco de Seguridad de Software) PCI SSC incluyen rigurosos requisitos de seguridad del software, el uso de software personalizado y a la medida que se desarrolla y mantiene de acuerdo con cualquiera de los estándares, puede ayudar a la entidad a cumplir con varios requisitos del Requisito 6 PCI DSS sin tener que realizar pruebas detalladas adicionales, y también puede admitir el uso del Enfoque Personalizado para otros requisitos. Para más información, consulte la Tabla 7.

***Nota**: Este apoyo al cumplimiento con el Requisito 6 se aplica solo al software desarrollado y gestionado específicamente de acuerdo con el Estándar de Software Seguro o el Estándar SLC Seguro; no se extiende a otro software o componentes del sistema en el ámbito del Requisito 6.*

Tabla 7. Aprovechamiento del Marco de Seguridad del Software PCI para cumplir con el Requisito 6

Requisitos de PCI DSS	¿Cómo se aplican los requisitos de PCI DSS al Software Desarrollado y Gestionado de acuerdo con el Estándar de Software Seguro?	¿Cómo se aplican los requisitos de PCI DSS al Software Desarrollado y Gestionado de acuerdo con el Estándar SLC Seguro?
6.1 Los procesos y mecanismos para realizar las actividades del Requisito 6 están definidos y comprendidos.	Los requisitos/objetivos PCI DSS se aplican como de costumbre.	
6.2 El software a medida y personalizado se desarrolla de forma segura.	El requisito 6.2.4 PCI DSS se puede considerar adecuado para aquel software que ha sido desarrollado y gestionado de acuerdo con el Estándar de Software Seguro.	El requisito 6.2 PCI DSS se puede considerar adecuado para el software desarrollado y gestionado de acuerdo con el Estándar SLC Seguro.
6.3 Las vulnerabilidades de seguridad se identifican y abordan de inmediato.	Los requisitos/objetivos PCI DSS se aplican como de costumbre. El software desarrollado y gestionado de acuerdo con el Estándar SLC Seguro puede admitir el enfoque personalizado para los objetivos del Requisito 6.3. Si bien el uso de software desarrollado y gestionado de acuerdo con el Estándar SLC Seguro brinda la garantía de que el proveedor ofrece parches de seguridad y actualizaciones de software de manera oportuna, **la entidad conserva la responsabilidad** de garantizar que los parches y las actualizaciones se instalen de acuerdo con los requisitos de PCI DSS.	

Requisitos de PCI DSS	¿Cómo se aplican los requisitos de PCI DSS al Software Desarrollado y Gestionado de acuerdo con el Estándar de Software Seguro?	¿Cómo se aplican los requisitos de PCI DSS al Software Desarrollado y Gestionado de acuerdo con el Estándar SLC Seguro?
6.4 Las aplicaciones web públicas están protegidas contra ataques.	Los requisitos/objetivos PCI DSS se aplican como de costumbre.	
6.5 Los cambios en todos los componentes del sistema se gestionan de forma segura.	Los requisitos/objetivos PCI DSS se aplican como de costumbre. El software desarrollado y gestionado de acuerdo con el Estándar SLC Seguro puede admitir el enfoque personalizado para los objetivos del Requisito 6.5. Aunque el uso de software desarrollado y gestionado de acuerdo con el Estándar SLC Seguro proporciona la garantía de que el proveedor sigue los procedimientos de gestión de cambios durante el desarrollo del software y las actualizaciones relacionadas, **la entidad conserva la responsabilidad** de garantizar que el software y otros cambios en los componentes del sistema se implementan en su entorno de producción de acuerdo con los requisitos de PCI DSS.	

Uso de software personalizado y a la medida gestionado por un proveedor calificado de SLC Seguro

Al validar el uso de software desarrollado y gestionado por un proveedor calificado de SLC Seguro para cumplir con el Requisito 6.2 PCI DSS y respaldar el Enfoque Personalizado para los Requisitos 6.3 y 6.5, el asesor debe confirmar que se cumpla con lo siguiente:

- El proveedor de software está incluido en la lista PCI SCC de Proveedores Calificados de SLC Seguro, es decir, que la validación no haya caducado.
- El software se ha desarrollado y se mantiene utilizando las prácticas de gestión del ciclo de vida del software que se evaluaron como parte de la validación del proveedor de software.
- La entidad cumple con las directrices de implementación proporcionadas por el Proveedor Calificado de SLC Seguro.

Uso de software personalizado y a la medida desarrollado de acuerdo con el Estándar de SLC Seguro

Las entidades que desarrollan internamente software para su uso exclusivo o que desarrollan software para uso de una sola entidad, pueden optar por contratar a un Asesor de SLC Seguro para que Evalúe sus prácticas de gestión del ciclo de vida del software de acuerdo con el Estándar de SLC Seguro. El Asesor de SLC Seguro documentará los resultados de la evaluación en un Informe de Cumplimiento de SLC Seguro (ROC) y un Certificado de Cumplimiento de SLC Seguro (AOC).

El software que se desarrolla y gestiona siguiendo las prácticas de gestión del ciclo de vida del software proporciona el mismo apoyo para el Requisito 6 PCI DSS que el software desarrollado y gestionado por un Proveedor Calificado de SLC Seguro, si esas prácticas fueron

evaluadas por un Asesor de SLC Seguro y se confirmó que cumplían con los requisitos del Estándar de SLC Seguro, con los resultados documentados en un ROC y un AOC de SLC Seguro.

Validación del uso del Estándar de SLC Seguro

Al validar el uso de software desarrollado y gestionado de acuerdo con el Estándar de SLC Seguro para cumplir el requisito 6.2 PCI DSS y apoyar el enfoque personalizado para los requisitos 6.3 y 6.5, el asesor debe confirmar que se cumpla con lo siguiente:

- Las prácticas de gestión del ciclo de vida del software han sido evaluadas por un Asesor de SLC Seguro y se ha confirmado que cumplen con todos los requisitos del Estándar de SLC Seguro, con los resultados documentados en un Informe de Conformidad (ROC) de SLC Seguro y en un Certificado de Conformidad (AOC) de SLC Seguro.
- El software fue desarrollado y gestionado utilizando las prácticas de gestión del ciclo de vida del software cubiertas por la evaluación del SLC Seguro.
- Una evaluación completa de SLC Seguro de las prácticas de gestión del ciclo de vida del software se completó dentro de los 36 meses previos. Además, si la evaluación completa del SLC Seguro más reciente tuvo lugar hace más de 12 meses, el desarrollador/proveedor debió proporcionar un Certificado Anual durante los 12 meses anteriores que confirma la adhesión continua al Estándar de SLC Seguro para las prácticas de gestión del ciclo de vida del software en uso.

Validación del uso del Estándar de Software Seguro

Al validar el uso del software desarrollado y gestionado de acuerdo con el Estándar de Software Seguro para cumplir con el Requisito 6.2.4 PCI DSS y apoyar el enfoque personalizado para los requisitos 6.3 y 6.5, el asesor debe confirmar que se cumple con lo siguiente:

- La evaluación del software seguro fue conducida por un asesor de Software Seguro y se confirmó que cumple con todos los requisitos del Estándar de Software Seguro, con resultados documentados en un Informe de Validación de Software Seguro (ROV) y en un Certificado de Validación de Software Seguro (AOV).
- El software se desarrolló y se gestiona utilizando las prácticas de gestión del ciclo de vida del software que se incluyeron en la evaluación del software seguro.
- En los 36 meses anteriores se realizó una evaluación completa del software seguro. Además, si la última evaluación completa del Software Seguro tuvo lugar hace más de 12 meses, el desarrollador/proveedor proporcionó un Certificado Anual en los 12 meses anteriores que confirma la adhesión continua al Estándar de Software Seguro.

Anexo G Glosario de Términos, Abreviaturas y Acrónimos PCI DSS

Término	Definición
Acceso Administrativo	Privilegios elevados o aumentados concedidos a una cuenta para que esa cuenta gestione sistemas, redes y/o aplicaciones. El acceso administrativo puede asignarse a la cuenta de un individuo o a una cuenta integrada en el sistema. Las cuentas con acceso administrativo suelen denominarse "*superusuario*", *"root*", "administrador", "*sysadmin*" o "supervisor-estado", según el sistema operativo y la estructura organizativa en particular.
Acceso Sin Consola	Acceso lógico a un componente del sistema que se produce a través de una interfaz de red en lugar de una conexión física directa al componente del sistema. El acceso sin consola incluye el acceso desde redes locales/internas, así como el acceso desde redes externas o remotas.
Adquisidor	También denominado "banco comercial", "banco adquirente" o "institución financiera adquirente". Entidad, normalmente una institución financiera, que procesa las transacciones de tarjetas de pago para los comerciantes y es definida por una marca de pago como adquirente. Los adquirentes están sujetos a los Estándares y procedimientos de las marcas de pago en relación con el cumplimiento de los comerciantes. Ver Procesador de Pagos.
AES	Acrónimo de "*Advanced Encryption Standard*"(Estándar de Cifrado Avanzado). Ver Criptografía robusta.
Alcance	Proceso de identificación de todos los componentes, personas y procesos del sistema que se incluirán en una evaluación PCI DSS. Ver "Alcance de los Requisitos de PCI DSS" en Requisitos de PCI DSS y Procedimientos de Evaluación de Seguridad.
Algoritmo Criptográfico	También denominado "algoritmo de cifrado". Proceso matemático reversible claramente especificado que se utiliza para transformar datos no cifrados en datos cifrados, y viceversa. Ver Criptografía robusta.
Algoritmo de Cifrado	Ver Algoritmo Criptográfico.
Análisis de Riesgo Específicos	A los efectos PCI DSS, un análisis de riesgo que se centra en un requisito de interés específico PCI DSS, ya sea porque el requisito permite flexibilidad (por ejemplo, en cuanto a la frecuencia) o, para el Enfoque Personalizado, para explicar cómo la entidad evaluó el riesgo y determinó que el control personalizado cumple con el objetivo de un requisito de PCI DSS.
Antimalware	Software diseñado para detectar y eliminar, bloquear o contener diversas formas de software malicioso.
AOC	Acrónimo de "*Attestation of Compliance*" (Atestación de Cumplimiento). El AOC es el formulario oficial PCI SCC para que los comerciantes y los proveedores de servicios den fe de los resultados de una evaluación PCI DSS, tal como se documenta en un Cuestionario de Autoevaluación (SAQ) o en un Informe de Cumplimiento (ROC).
Aplicación	Incluye todos los programas de software o grupos de programas adquiridos, personalizados y a medida, incluyendo las aplicaciones internas y externas (por ejemplo, web).

Término	Definición
Aplicación Web	Una aplicación a la que generalmente se ingresa a través de un navegador web o a través de servicios web. Las aplicaciones web pueden estar disponibles a través de Internet o de una red interna privada.
Área Sensible	Un área sensible suele ser un subconjunto del CDE y es cualquier área que alberga sistemas considerados críticos para el CDE. Esto incluye centros de datos, salas de servidores, salas administrativas en establecimientos minoristas y cualquier área que concentre o agregue almacenamiento, procesamiento o transmisión de datos de titulares de tarjetas. Las áreas sensibles también incluyen áreas que albergan sistemas que administran o mantienen la seguridad del CDE (por ejemplo, aquellas que brindan controles de seguridad de la red o que administran la seguridad física o lógica). Esto excluye las áreas donde solo hay terminales de punto de venta, como las áreas de caja en una tienda minorista o los centros de llamadas donde los agentes reciben pagos.
ASV	Acrónimo de "*Approved Scanning Vendor*". (Proveedor Aprobado de Análisis). Empresa aprobada por PCI SCC para desarrollar servicios externos de escaneo de vulnerabilidades.
Autenticación	Proceso de verificación de identidad de un individuo, dispositivo o proceso. La autenticación suele producirse con uno o más factores de autenticación. Ver Cuenta, Credencial de Autenticación, y Factor de Autenticación.
Autenticación Multifactorial	Método de autenticación de un usuario mediante el cual se verifican al menos dos factores. Estos factores incluyen algo que el usuario tiene (como una tarjeta inteligente *o dongle),* algo que el usuario conoce (como una contraseña, frase de contraseña o PIN) o algo que el usuario es o hace (como huellas dactilares y otros elementos biométricos).
Autorización	En el contexto del control de acceso, la autorización es la concesión de acceso u otros derechos a un usuario, programa o proceso. La autorización define lo que un individuo o programa puede hacer después de una autenticación exitosa. En el contexto de una transacción con tarjeta de pago, la autorización se refiere al proceso de autorización, que se completa cuando un comerciante recibe una respuesta de la transacción (por ejemplo, una aprobación o un rechazo).
BAU	Acrónimo de "Business as Usual". (Procesos Habituales).
Bloque de PIN	Bloque de datos utilizado para encapsular un PIN durante el procesamiento. El formato de bloque de PIN define el contenido del bloque de PIN y cómo se procesa para recuperar el PIN. El bloque de PIN se compone del PIN, la longitud del PIN, y puede contener los datos PAN (o un truncamiento del mismo) según el formato de bloque PIN ISO aprobado que se utilice.
CIS	Acrónimo de "Center for Internet Security". (Centro de Seguridad en Internet).
CDE	Acrónimo de "*Cardholder Data Environment."* (Entorno de Datos del Tarjetahabiente). El CDE está compuesto por: • Los componentes del sistema, las personas y los procesos que almacenan, procesan o transmiten datos del titular de la tarjeta o datos sensibles de autenticación y/o • Componentes del sistema que pueden no almacenar, procesar o transmitir CHD/SAD pero que tienen una conectividad sin restricciones con componentes del sistema que almacenan, procesan o transmiten CHD/SAD.
CERT	Acrónimo de "*Computer Emergency Response Team*". (Equipo de Respuesta ante Emergencias Informáticas).

Término	Definición
Cifrado a Nivel de Archivo	Técnica o tecnología (ya sea de software o hardware) para cifrar el contenido completo de archivos específicos. Como alternativa, ver Cifrado de Disco y Cifrado de Base de Datos a Nivel de Columna.
Cifrado de Disco	Técnica o tecnología (de software o hardware) para cifrar todos los datos almacenados en un dispositivo (por ejemplo, un disco duro o una unidad flash). Alternativamente, el Cifrado a Nivel de Archivo o de la Base de Datos a Nivel de Columna se utiliza para cifrar el contenido de archivos o columnas específicas.
Clave Criptográfica	Parámetro utilizado junto con un algoritmo criptográfico que se utiliza para operaciones como: • Transformar datos no cifrados en datos de texto cifrado, • Transformación de datos de texto cifrado a datos no cifrados. • Una firma digital calculada a partir de datos, • Verificar una firma digital calculada a partir de datos, • Un código de autenticación calculado a partir de datos, o • Un acuerdo de intercambio de un secreto compartido. Ver Criptografía robusta.
Codificación Segura	El proceso de creación e implementación de aplicaciones que son resistentes a la manipulación y/o situaciones comprometidas.
Código de Servicio	Valor de tres o cuatro dígitos en la banda magnética que sigue a la fecha de caducidad de la tarjeta de pago en los datos de seguimiento. Se utiliza para varias cosas, como definir atributos del servicio, diferenciar entre intercambio internacional y nacional o identificar restricciones de uso.
Código de Verificación de Tarjeta	También conocido como Código o Valor de Validación de Tarjeta, o Código de Seguridad de la Tarjeta. A efectos PCI DSS, es el valor de tres o cuatro dígitos impresos en el anverso o el reverso de una tarjeta de pago. Puede denominarse CAV2, CVC2, CVN2, CVV2 o CID según las Marcas de Pago Participantes. Para más información, póngase en contacto con las Marcas de Pago Participantes.
Comerciante	A los efectos PCI DSS, un comerciante se define como cualquier entidad que acepta tarjetas de pago con los logotipos de cualquier Marca de Pago Participante en PCI SCC como pago por bienes y/o servicios. Un comerciante que acepta tarjetas de pago como pago de bienes y/o servicios también puede ser un proveedor de servicios, si los servicios vendidos resultan en el almacenamiento, procesamiento o transmisión de datos del titular de la tarjeta en nombre de otros comerciantes o proveedores de servicios. Por ejemplo, un ISP es un comerciante que acepta tarjetas de pago para la facturación mensual, pero también es un proveedor de servicios si acoge a los comerciantes como clientes.
Comercio Electrónico (web)	Es el proceso de compra y venta de productos por medios electrónicos, principalmente a través de Internet.
Componentes del Sistema	Cualquier dispositivo de red, servidor, dispositivo informático, componente virtual o software incluido o conectado al CDE, o que pueda afectar la seguridad del CDE.

Término	Definición
Comprometer	También denominado "datos comprometidos" o "violación de datos". Intrusión en un sistema informático en el que se sospecha la divulgación/robo, modificación o destrucción no autorizada de los datos de titulares de tarjetas.
Conexión de Red	Una ruta de comunicación lógica, física o virtual entre dispositivos que permiten la transmisión y recepción de paquetes de capa de red.
Conocimiento Compartido	Método por el cual dos o más entidades por separado tienen componentes clave o claves compartidas que individualmente no transmiten ningún conocimiento de la clave criptográfica resultante.
Consola	Pantalla y/o teclado conectado directamente que permiten el acceso y control a un servidor, ordenador central u otro tipo de sistema. Ver Acceso Sin Consola.
Consumidor	Titular de una tarjeta que compra bienes, servicios o ambos.
Contraseña / Frase de paso	Una cadena de caracteres que sirve como factor de autenticación para un usuario o cuenta.
Contraseña Predeterminada	Contraseña en la administración del sistema, usuario o cuentas de servicio predeterminadas en un sistema, aplicación o dispositivo; normalmente vinculada a la cuenta predeterminada. Las cuentas y contraseñas predeterminadas son publicadas y bien conocidas, y por lo tanto, fáciles de adivinar.
Control de Cambios	Procesos y procedimientos para revisar, probar y aprobar los cambios en los sistemas y en el software a fin de determinar su impacto antes de la implementación.
Control de Ingreso Físico	Mecanismos que limitan el acceso a un espacio físico o ambiente sólo para personas autorizadas. Ver Control de Ingreso Lógico
Control de Ingreso Lógico	Mecanismos que limitan la disponibilidad de información o recursos de procesamiento de información solo a personas autorizadas o aplicaciones. Ver Control de Ingreso Físico
Control Dual	Proceso de utilizar dos o más entidades separadas (usualmente personas) que operan de forma concertada para proteger funciones o información confidencial. Ambas entidades son igualmente responsables de la protección física de los materiales implicados en las operaciones vulnerables. Ninguna persona puede ingresar o utilizar los materiales (por ejemplo, la clave criptográfica). En el caso de la generación, el transporte, la carga, el almacenamiento y la recuperación manual de claves, el control dual requiere dividir el conocimiento de la clave entre las entidades. Ver Conocimiento Compartido.
Controles Compensatorios	Ver los Anexos B y C de los Requisitos de PCI DSS y los Procedimientos de Evaluación de la Seguridad.
Controles de Seguridad de Red (NSC)	*Firewalls* y otras tecnologías de seguridad de red que actúan como puntos de cumplimiento de políticas de red. Los NSC normalmente controlan el tráfico de red entre dos o más segmentos de red físicos o lógicos (o sub-redes) basados en políticas o reglas predefinidas.

Término	Definición
Credencial de Autenticación	Combinación del ID de usuario o cuenta ID, más el/los factor/es de autenticación utilizados para autenticar a un individuo, dispositivo o proceso. Ver Cuenta y Factor de Autenticación.
Criptografía Sólida	La criptografía es un método para proteger los datos a través de un proceso de cifrado reversible, y es un fundamento rudimentario utilizado en muchos protocolos y servicios de seguridad. La criptografía sólida se basa en algoritmos probados y aceptados por la industria junto con longitudes de clave que brindan un mínimo de 112 bits de fortaleza de clave efectiva y prácticas adecuadas de administración de claves. La fuerza efectiva de la clave puede ser más corta que la longitud real de "bits" de la clave, lo que puede llevar a que los algoritmos con claves más amplias brinden menos protección que los algoritmos con clave más pequeñas, pero efectivos más grandes. Se recomienda que todas las implementaciones nuevas utilicen un mínimo de 128 bits de fuerza de clave efectiva. Ejemplos de referencias de la industria sobre algoritmos criptográficos y longitudes de clave incluyen: • Publicación especial NIST 800-57 Parte 1, • BSI TR-02102-1, • ECRYPT-CSA D5.4 *Algorithms, Key Size and Protocols Report* (2018), y • ISO/IEC 18033-3:2010/Amd 1:2021 Tecnología de la información. Técnicas de seguridad. Algoritmos de cifrado. Parte 3:
Criptoperíodo	El periodo de tiempo durante el cual una clave criptográfica puede ser utilizada para su propósito definido. A menudo se define en términos del período durante el cual la clave está activa y/o la cantidad de texto cifrado que ha sido producido por la clave, y de acuerdo con las mejores prácticas y directrices de la industria (por ejemplo, Publicación Especial del NIST 800-57).
Cuenta	También denominada "ID de usuario", "ID de cuenta" o "ID de aplicación". Se utiliza para identificar a un individuo o proceso en un sistema informático. *Ver Credenciales de Autenticación y Factor de Autenticación.*
Cuenta Predeterminada	Cuenta de inicio de sesión predeterminada en un sistema, aplicación o dispositivo para permitir el acceso inicial cuando el sistema se pone en servicio por primera vez. El sistema también puede generar cuentas adicionales predeterminadas como parte del proceso de instalación.
Cuentas de Aplicación y de Sistema.	También denominadas "cuentas de servicio". Cuentas que ejecutan procesos o realizan tareas en un sistema informático o en una aplicación. Estas cuentas suelen tener privilegios elevados requeridos para realizar tareas o funciones especializadas y no suelen ser cuentas utilizadas por un individuo.
Custodio Clave	Posición que se confía a personas responsables de realizar tareas de administración esenciales que involucran claves secretas y/o privadas, claves compartidas o componentes clave en nombre de una entidad.
CVSS	Acrónimo de "*Common Vulnerability Scoring System*". (Sistema de Puntaje de Vulnerabilidad Común). Consulte la Guía del Programa ASV para más información.

Término	Definición
Datos Confidenciales de Autenticación	Información relacionada con la seguridad para autenticar las transacciones de los titulares de tarjetas y/o autorizar transacciones con tarjetas de pago. Esta información incluye, entre otros, códigos/valores de verificación de validación de tarjetas, datos de pista completo (de banda magnética o equivalente en un chip), PIN y bloques de PIN.
Datos de Banda Magnética	Ver Datos de Pista
Datos de la Cuenta	Los datos de cuentas consisten en datos del titular de la tarjeta y/o información confidencial de autenticación. Ver Datos de Titulares de Tarjetas y Datos Confidenciales de Autenticación.
Datos de Pista	También denominados "datos de pista completos" o "datos de banda magnética". Datos codificados en la banda magnética o chip utilizado para la autenticación y/o la autorización durante las transacciones de pago. Puede ser la imagen de la banda magnética en un chip o los datos completos en la banda magnética.
Datos del Titular de la Tarjeta	Como mínimo, los datos del titular de la tarjeta consisten en los datos PAN completos. Los datos del titular de la tarjeta también pueden consistir en datos PAN completos más cualquiera de los siguientes datos: nombre del titular de la tarjeta, fecha de caducidad y/o código de servicio. Ver Datos Confidenciales de Autenticación para conocer otros elementos de datos que podrían transmitirse o procesarse (pero no almacenarse) como parte de una operación de pago.
Datos No Cifrados	Datos desencriptados.
Diagrama de Flujo de Datos	Diagrama que muestra cómo fluyen los datos a través de una aplicación, sistema o red.
Diagrama de Red	Un diagrama que muestra los componentes del sistema y las conexiones dentro de un entorno de red.
DMZ	Abreviatura para "zona desmilitarizada". Sub-red física o lógica que proporciona una capa adicional de seguridad a la red privada interna de una organización.
DNS	Acrónimo *de "Domain Name System".* (Sistema de Nombre de Dominio).
ECC	Acrónimo de "*Elliptic Curve Cryptography."* (Criptografía de Curva Elíptica"). Ver Criptografía robusta.
Emisor	También denominado "banco emisor" o "institución financiera emisora". Entidad que emite tarjetas de pago o realiza, facilita o respalda los servicios de emisión, incluyendo, entre otros, los bancos emisores y los procesadores emisores.
Encriptación	Transformación (reversible) de datos mediante un algoritmo criptográfico para producir un texto cifrado, es decir, para ocultar el contenido informativo de los datos. Ver Criptografía robusta.
Encriptación de base de datos	Técnica o tecnología (ya sea de software o hardware) para cifrar el contenido de una columna específica de una base de datos frente al contenido completo de toda la base de datos. Como alternativa, ver Cifrado de Disco y Cifrado a nivel de archivo.

Término	Definición
Enfoque Definido	Véase "Enfoques para la Implementar y Validar PCI DSS" en Requisitos de PCI DSS y Procedimientos de Evaluación de la Seguridad.
Enfoque Personalizado	Véase "Enfoques para la Implementar y Validar PCI DSS" en Requisitos de PCI DSS y Procedimientos de Evaluación de la Seguridad.
Enmascaramiento	Método para ocultar un segmento de datos PAN cuando se muestran o imprimen. El enmascaramiento se utiliza cuando no existe una necesidad empresarial de ver toda la información de datos PAN. El enmascaramiento se relaciona con la protección de datos PAN cuando se muestra en pantallas, recibos en papel, impresiones, etc. Ver Truncamiento para la protección de datos PAN cuando se almacenan, procesan o transmiten electrónicamente.
Entidad	Término utilizado para denominar a la corporación, organización o negocio que se somete a una evaluación PCI DSS.
Evaluación de Riesgos	Proceso que abarca toda la empresa para identificar recursos y amenazas importantes al sistema; cuantifica las exposiciones a pérdidas (es decir, el potencial de pérdidas) en función de las frecuencias estimadas y los costos de ocurrencia; y (opcionalmente) recomienda cómo asignar recursos a las contramedidas para minimizar la exposición total. Ver Análisis de Riesgos Específicos.
Evento de Seguridad	Una ocurrencia que una organización considera que tiene posibles implicaciones de seguridad para un sistema o su entorno. En el contexto PCI DSS, los eventos de seguridad identifican actividades sospechosas o anómalas.
Factor de Autenticación	Elemento utilizado para probar o verificar la identidad de un individuo o de un proceso en un sistema informático. La autenticación típicamente ocurre con uno o más de los siguientes factores de autenticación: • Algo que se conoce, como una contraseña o frase de paso. • Algo que se es, como un elemento biométrico. • Algo que se tiene, como un dispositivo *token* o una tarjeta inteligente. La ID (o cuenta) y el factor de autenticación se consideran conjuntamente credenciales de autenticación. “Ver Cuenta y Credencial de Autenticación.”
Factor de Forma de Tarjeta de Pago	Incluye tarjetas de pago físicas, así como dispositivos con funcionalidad que emulan una tarjeta de pago para iniciar una transacción de pago. Ejemplos de dichos dispositivos incluyen, entre otros, teléfonos inteligentes, relojes inteligentes, pulseras de actividad física, llaveros y dispositivos portátiles como joyas.
Firewall	Tecnología de hardware y/o software que protege los recursos de la red del acceso no autorizado. Un *firewall* permite o deniega el tráfico informático entre redes con diferentes niveles de seguridad basándose en un conjunto de reglas y otros criterios.
Forense	También denominada "informática forense". En lo que respecta a la seguridad de la Información, es la aplicación de herramientas de investigación y técnicas de análisis para recopilar pruebas de los recursos informáticos con el fin de determinar la causa de situaciones de datos comprometidos. Las investigaciones sobre datos de pago comprometidos suelen ser realizadas por un Investigador Forense PCI (PFI).

Término	Definición
FTP	Acrónimo de *"File Transfer Protocol*". (Protocolo de Transferencia de Archivos). Protocolo de red utilizado para transferir datos de un computador a otro a través de una red pública como Internet. El FTP es ampliamente considerado un protocolo inseguro porque las contraseñas y el contenido de los archivos se envían sin protección y en texto no cifrado. El FTP puede implementarse de forma segura mediante SSH u otra tecnología.
Generación de Claves Criptográficas	La generación de claves es una de las funciones dentro de la gestión de claves. Los siguientes documentos proporcionan una guía reconocida sobre la generación adecuada de claves: • Publicación Especial NIST 800-133: Recomendación para la Generación de Claves Criptográficas. • ISO 11568-2 Servicios Financieros - Gestión de Claves (minoristas) - Parte 2: Códigos simétricos, su gestión de claves y ciclo de vida. – 4.3 Generación de Claves • ISO 11568-4 Servicios Financieros - Gestión de Claves (minoristas) - Parte 4: Criptosistemas Asimétricos - Gestión de claves y ciclo de vida. – 6.2 Fases del ciclo de vida de las claves - Generación • Consejo Europeo de Pagos EPC 342-08 Directrices sobre el Uso de Algoritmos y la Gestión de Claves. – 4.1.1 Generación de claves [para algoritmos simétricos] – 4.2.1 Generación de claves [para algoritmos asimétricos].
Gestión de Claves Criptográficas	Conjunto de procesos y mecanismos que respaldan el establecimiento y el mantenimiento de claves criptográficas, incluyendo la sustitución de claves antiguas por otras nuevas cuando sea necesario.
Hashing	Método de protección de datos que convierte los datos en un compendio de mensajes de longitud fija. *Hashing* es una función unidireccional (matemática) en la que un algoritmo no secreto toma cualquier mensaje de longitud arbitraria como entrada y produce una salida de longitud fija (generalmente llamada "código *hash*" o "resumen de mensaje"). Las funciones *hash* deben tener las siguientes propiedades: • Ser computacionalmente inviable para determinar la entrada original dada solo con el código *hash*, • Ser computacionalmente inviable encontrar dos entradas que den el mismo código *hash*.
***Hash* Criptográfico con Clave**	Una función *hash* que incorpora una clave secreta generada aleatoriamente para proporcionar resistencia a ataques de fuerza bruta e integridad de autenticación secreta. Los algoritmos *hashing* criptográficos en clave adecuados incluyen, entre otros, los siguientes: HMAC, CMAC y GMAC, con fuerza criptográfica efectiva de al menos 128 bits (NIST SP 800-131Ar2). Refiérase a los siguientes para obtener más información sobre HMAC, CMAC y GMAC, respectivamente: NIST SP 800-107r1, NIST SP 800-38B y NIST SP 800-38D). Véase NIST SP 800-107 (Revisión 1): Recomendación para Aplicaciones que Utilizan Algoritmos *Hash* Aprobados §5.3.

Término	Definición
HSM	Acrónimo de "Hardware Security Module". (Módulo de Seguridad de Hardware o Módulo de Seguridad de Host). Un dispositivo de hardware protegido física y lógicamente que proporciona un conjunto seguro de servicios criptográficos, utilizado para funciones de administración de claves criptográficas y/o el descifrado de datos de cuentas.
IDS	Acrónimo de *"Intrusion Detection System".* (Sistema de Detección de Intrusiones).
Independencia Organizacional	Una estructura organizativa que garantiza que no haya conflicto de interés entre la persona o el departamento que realiza la actividad y la persona o el departamento que evalúa la actividad. Por ejemplo, las personas que realizan evaluaciones están organizacionalmente separadas de la gestión del entorno que se evalúan.
Índice de *Token*	Un valor aleatorio de una tabla de valores aleatorios que corresponde a datos PAN determinados.
Ingreso Remoto	Ingreso a la red de una entidad desde una ubicación fuera de esa red. Un ejemplo de tecnología para el acceso remoto es una VPN.
Inicio de sesión interactivo	El proceso de una persona que proporciona credenciales de autenticación para iniciar sesión directamente en una aplicación o cuenta de un sistema.
IPS	Acrónimo de "*Intrusion Detection System*" (Sistema de Prevención de Intrusiones).
ISO	Acrónimo de "*International Organization for Standardization*" (Organización Internacional para la Estandarización).
LAN	Acrónimo de "*Local Area Network"* (Red de Área Local).
LDAP	Acrónimo de "*Lightweight Directory Access Protocol*." (Protocolo Ligero de Acceso a Directorios).
MAC	En criptografía, acrónimo de "*Message Authentication Code"* (código de autenticación de mensajes). Ver Criptografía robusta.
Marca de Pago	Una organización con tarjetas de pago de marca u otros factores en forma de tarjetas de pago. Las Marcas de Pago regulan dónde y cómo se utilizan las tarjetas de pago u otros factores de forma que llevan su marca o logotipo. Una marca de pago puede ser Marca de Pago Participante PCI SCC u otra marca de pago regional o global, esquema o red.
Marca de Pago Participante	También conocida como "marca de pago". Una marca de tarjeta de pago que, en el momento en cuestión, se admite formalmente como (o afiliada de) un miembro PCI SCC de conformidad con sus documentos rectores. Al momento de redactar este informe, las Marcas de Pago Participantes incluyen Miembros Fundadores y Miembros Estratégicos PCI SCC.
Medio	Material físico, incluidos, entre otros, dispositivos de almacenamiento electrónico, medios electrónicos extraíbles e informes en papel.
Medios Electrónicos Extraíbles	Medios que almacenan datos digitalizados que pueden eliminarse y/o transportarse fácilmente de un sistema informático a otro. Ejemplos de medios electrónicos extraíbles incluyen CD-ROM, DVD-ROM, unidades flash USB y discos duros externos/portátiles. En este contexto, los medios electrónicos extraíbles no incluyen unidades intercambiables en caliente, unidades de cinta utilizadas para copias de seguridad masivas u otros medios que normalmente no se utilizan para transportar datos desde una ubicación para su uso a otra.

Término	Definición
MO/TO	Acrónimo de "*Mail Order/Telephone Order"* (Orden-Postal/Orden Telefónica).
Monitoreo de la integridad de los archivos (FIM)	Una solución de detección de cambios que comprueba los cambios, adiciones y eliminaciones de los archivos críticos, y notifica cuando se detectan dichos cambios.
NAC	Acrónimo de "*Network Access Control."* (Control de Acceso de Red).
NAT	Acrónimo de "*Network Address Translation*." (Traducción de Direcciones de Red).
NIST	Acrónimo de "*National Institute of Standards and Technology."* (Instituto Nacional de Estándars y Tecnología). Agencia federal No-Reguladora dentro de los EE. UU. Administración de Tecnología del Departamento de Comercio.
Nivel de Columna	Técnica o tecnología (ya sea de *software o hardware*) para cifrar el contenido de una columna específica de una base de datos frente al contenido completo de toda la base de datos. Como alternativa, ver Cifrado de Disco y Cifrado a nivel de archivo.
NTP	Acrónimo de "*Network Time Protocol*." (Protocolo de Tiempo de Red).
Objeto de Nivel de Sistema	Todo lo que se requiera, en un componente del sistema, para su funcionamiento; incluyendo entre otros, archivos ejecutables y de configuración de aplicaciones, archivos de configuración del sistema, bibliotecas y archivos DLL estáticos y compartidos, archivos ejecutables del sistema, controladores de dispositivos y archivos de configuración de dispositivos, y componentes de terceros.
Oficial de Seguridad	Persona principal responsable de la seguridad de una entidad.
OWASP	Acrónimo de "*Open Web Application Security Project*." (Guía para proyectos de seguridad de aplicaciones web abiertas).
Página de Pago	Una interfaz de usuario basada en la web que contiene uno o más elementos de formularios destinados a capturar datos de cuenta de un consumidor o enviar datos de cuenta capturados. La página de pago se puede representar como cualquiera de los siguientes: • Un solo documento o instancia, • Un documento o componente desplegado en un marco en línea dentro de una página de impago. • Varios documentos o componentes, cada uno de los cuales contiene uno o más elementos de formulario contenidos en varios marcos en línea dentro de una página de impago.
PAN	Acrónimo de "*Personal Account Number"* (Número de Cuenta Principal). Número único de tarjeta de pago (tarjetas de crédito, débito o pre-pago, etc.) que identifica al emisor y al titular de la tarjeta cuenta.
Parche	Actualización de un software existente para agregar funciones o corregir un defecto.
PCI DSS	Acrónimo de "*Payment Card Industry Data Security Standard*". (Estándar de Seguridad de Datos de la Industria de las Tarjetas de Pago).

Término	Definición
Personal	Empleados de tiempo medio y completo, empleados temporales, contratistas y consultores con responsabilidades de seguridad para proteger los datos cuentas o que puedan afectar la seguridad de los datos de cuentas.
PIN	Acrónimo de "*Personal Identification Number"* (Número de Identificación Personal).
POI	Acrónimo de "*Point of Interaction*" (Punto de Interacción), el punto inicial donde se leen los datos de una tarjeta.
Privilegios Básicos	El nivel mínimo de privilegios necesarios para desempeñar los roles y responsabilidades en un puesto laboral.
Procesador de Pagos	A veces se denomina "pasarela de pago" o "proveedor de servicios de pago (PSP)". La entidad comprometida con un comerciante o con otra entidad para manejar la tarjeta de pago en su nombre. Ver Adquirentes.
Productos de negocios disponibles (COTS)	Descripción de los artículos en stock que no están específicamente personalizados o diseñados para un cliente o usuario específico y que se encuentran fácilmente disponibles para su uso.
Proveedor de Servicio	La entidad que no es una marca para realizar pagos, directamente involucrada en el procesamiento, almacenaje, o transmisión de información del tarjeta-habiente en nombre de otra entidad. Esto incluye pasarelas de pago, proveedores de servicios de pago (PSP) y organizaciones de ventas independientes (ISO). Esto también incluye a las compañías que proporcionan los servicios que controlan o que podrían impactar la seguridad de los datos del tarjeta-habiente. Los ejemplos incluyen a los proveedores de servicios gestionados que proporcionan los *firewalls* gestionados, IDS y otros servicios como los proveedores de hosting y otras entidades. Si una entidad proporciona un servicio que involucra solo la provisión del acceso a la red pública; tal como una compañía de telecomunicaciones que proporciona solo el enlace de comunicación, la entidad no se consideraría como un proveedor de servicios para ese servicio (a pesar de que se puedan considerar como un proveedor de servicios para otros servicios). Ver Proveedor de *Servicios Multiusuario y Proveedor de Servicios de Terceros*.
Proveedor de Servicios de Terceros (TPSP)	Cualquier tercero que actúe como proveedor de servicios en nombre de una entidad. Ver Proveedor de servicios Multiusuario y Proveedor de Servicios.
Proveedor de Servicios Multiusuario	Un tipo de Proveedor de Servicios de Terceros que ofrece servicios en los que los clientes comparten recursos del sistema (tales como servidores físicos o virtuales), infraestructura, aplicaciones (incluyendo el Software como Servicio *(SaaS)*) y/o bases de datos, con el acceso a estos recursos o servicios controlados lógicamente o dividido para mantener los recursos contenidos y los datos aislados entre los distintos clientes. Ver Proveedor de Servicios y Proveedor de Servicios Externo.
QIR	Acrónimo de "*Qualified Integrators and Resellers"* (Integrador o Revendedor Calificado). Para más información consulte la Guía del Programa QIR en el sitio web PCI SCC.
QSA	Acrónimo de *"Qualified Security Assessor*" (Asesor de Seguridad Calificado). Los QSA están calificados por PCI SCC para realizar evaluaciones PCI DSS in situ. Refiérase a los Requisitos de Calificación de QSA para obtener detalles sobre los requisitos para empresas y empleados de QSA.

Término	Definición
Red Confiable	Red de una entidad que está dentro de la capacidad de control o gestión de la entidad y que cumple con los requisitos aplicables PCI DSS.
Red No Confiable	Cualquier red que no cumpla con la definición de una "red confiable".
Registro	Ver Registro de Auditoría.
Registro de Auditoría	También denominado "pista de auditoría". Registro cronológico de las actividades del sistema. Proporciona un rastro verificable de forma independiente, suficiente para permitir la reconstrucción, la revisión y el estudio de la secuencia de entornos y actividades que rodean o conducen a la operación, a un procedimiento o a un evento en una transacción, desde el inicio hasta los resultados finales.
ROC	Acrónimo de “Report on Compliance.” (Informe de Cumplimiento). Herramienta para la emisión de informes utilizada para documentar resultados detallados de la evaluación PCI DSS de una entidad.
RSA	Algoritmo para el cifrado de claves públicas. Ver Criptografía robusta.
SAD	Acrónimo de “*Sensitive Authentication Data.”* (Datos Confidenciales de Autenticación).
SAQ	Acrónimo de “*Self-Assessment Questionnaire*“ (Cuestionario de Auto-Evaluación”) Herramienta de emisión de informes utilizada para documentar los resultados de la autoevaluación PCI DSS de una entidad.
Scripts de Página de Pago	Cualquier comando o instrucción de lenguaje de programación en una página de pago que sea procesada y/o interpretada por el navegador de un consumidor, incluidos los comandos o instrucciones que interactúan con el modelo de objeto de documento de una página. Ejemplos de lenguajes de programación son JavaScript y VB script; ni los lenguajes de marcado (por ejemplo, HTML) ni las reglas de estilo (por ejemplo, CSS) son lenguajes de programación.
Segmentación	También se conoce como "segmentación de la red" o "aislamiento". La segmentación aísla los componentes del sistema que almacenan, procesan o transmiten datos del titular de la tarjeta de los sistemas que no lo hacen. Ver "Segmentación" en los Requisitos de PCI DSS y Procedimientos de Evaluación de Seguridad.
Separación de Tareas	Práctica de dividir los pasos de una función entre varios individuos, para evitar que un solo individuo altere el proceso.
Servicios de Emisión	Los ejemplos de servicios de emisión incluyen, entre otros, la autorización y personalización de tarjetas.
Servidor de Re-direccionamiento	Un servidor que redirige el navegador de un cliente desde el sitio web de un comerciante a una ubicación diferente para el procesamiento del pago durante una transacción de comercio electrónico.
Sistema de Gestión de Claves	Una combinación de hardware y software que provee un enfoque integrado para generar, distribuir o administrar claves criptográficas para dispositivos y aplicaciones.

Término	Definición
Sistemas Críticos	Sistema o tecnología que la entidad considera de especial importancia. Por ejemplo, un sistema crítico puede ser esencial para el desempeño de una operación comercial o para que se mantenga una función de seguridad. Algunos ejemplos de sistemas críticos suelen ser los sistemas de seguridad, los dispositivos y sistemas de cara al público, las bases de datos y los sistemas que almacenan, procesan o transmiten datos de los titulares de tarjetas.
Skimmer de tarjetas	Dispositivo físico, a menudo acoplado a un dispositivo legítimo de lectura de tarjetas, diseñado para capturar y/o almacenar ilegítimamente la información de una tarjeta de pago.
SNMP	Acrónimo de "*Simple Network Management Protocol*" (Protocolo Simple de Administración de Red).
Software a la Medida y Personalizado	El software a la medida es desarrollado para la entidad por un tercero en nombre de la entidad según sus especificaciones. El software personalizado es desarrollado por la entidad para su propio uso.
Software de Terceros	Software adquirido por una entidad, pero no desarrollado expresamente para ella. Puede ser de código abierto, *freeware, shareware* o comprado.
SQL	Acrónimo de "*Structured Query Language"* (Lenguaje de Consulta Estructurado).
SSH	Abreviatura de "*Secure Shell".*
SSL	Acrónimo de "*Secure Sockets Layer"* (Capa de Sockets Seguros).
Tarjetas de Pago	A los efectos PCI DSS, cualquier factor de forma de tarjeta de pago que lleve el logotipo de cualquier Marca de Pago.
TDES	Acrónimo de "*Triple Data Encryption Standard."* (Estándar de Cifrado de Datos Triple). También conocido como "3DES" o "Triple DES".
Telnet	Abreviatura de "protocolo de red telefónica".
Terminal de Pago Virtual	En el contexto del Cuestionario de Autoevaluación (SAQ) C-VT, una terminal de pago virtual es un acceso basado en un navegador web a un sitio web de adquirente, procesador o proveedor de servicios de terceros para autorizar transacciones con tarjetas de pago, donde el comerciante ingresa manualmente los datos de la tarjeta de pago a través de un navegador web. A diferencia de los terminales físicos, los terminales de pago virtuales no leen los datos directamente de una tarjeta de pago. Debido a que las transacciones con tarjeta de pago se ingresan manualmente, los terminales de pago virtuales generalmente se usan en lugar de los terminales físicos en entornos de negocios con bajos volúmenes de transacciones.
Titular de la tarjeta (Tarjetahabiente)	Cliente al que se emite una tarjeta de pago o cualquier persona autorizada a utilizar la tarjeta de pago.
TLS	Acrónimo de "*Transport Layer Security*" (Seguridad de la Capa de Transporte).

Término	Definición
Token	En el contexto de autenticación y control de acceso, un *token* es un valor proporcionado por hardware o software que funciona con un servidor de autenticación o VPN para realizar una autenticación dinámica o multifactorial.
Truncamiento	Método para hacer ilegible los datos PAN completos mediante la eliminación de un segmento de los datos PAN. El truncamiento se relaciona con la protección de datos PAN cuando se almacenan, procesan o transmiten electrónicamente. Ver Enmascaramiento para la protección de datos PAN cuando se muestra en pantallas, recibos en papel, etc.
Usuario Privilegiado	Cualquier cuenta de usuario con privilegios de acceso superiores a los básicos. Por lo general, estas cuentas tienen privilegios elevados o aumentados con más derechos que una cuenta de usuario estándar. Sin embargo, el alcance de los privilegios en diferentes cuentas privilegiadas puede variar mucho según la organización, la función del cargo y la tecnología en uso.
Virtualización	La abstracción lógica de los recursos informáticos a partir de restricciones físicas y/o lógicas. Una abstracción común se conoce como máquinas virtuales o VM, que toma el contenido de una máquina física y le permite operar en un hardware físico diferente y/o junto con otras máquinas virtuales en el mismo hardware físico. Otras abstracciones comunes incluyen, entre otros, contenedores, computación sin servidor o micro-servicios.
VPN	Acrónimo de "*Virtual Private Network*" (Red Privada Virtual).
Vulnerabilidad	Defecto o debilidad que, si se explota, puede resultar en el compromiso intencional o no intencional del sistema.