



**Normas de Seguridad de Datos
de la Industria de Tarjetas de Pago (PCI DSS)
Exploración de PCI DSS**

Comprensión del objetivo de los requisitos

Versión 1.2

Octubre de 2008

Modificaciones realizadas a los documentos

<i>Fecha</i>	<i>Versión</i>	<i>Descripción</i>
<i>1.º de octubre de 2008</i>	<i>1.2</i>	<i>Alinear el contenido con las nuevas PCI DSS versión 1.2 e implementar cambios menores observados desde la versión 1.1. original.</i>

Índice

Modificaciones realizadas a los documentos.....	i
Prefacio	iii
Elementos de los datos del titular de la tarjeta y de los datos confidenciales de autenticación.....	1
<i>Ubicación de los datos de los titulares de tarjetas y de los datos confidenciales de autenticación</i>	<i>2</i>
<i>Datos de la pista 1 y pista 2</i>	<i>3</i>
Guía relacionada para las Normas de Seguridad de Datos de la PCI.....	4
Guía para los requisitos 1 y 2: Desarrollar y mantener una red segura	5
<i>Requisito 1: Instale y mantenga una configuración de firewall para proteger los datos de los titulares de las tarjetas</i>	<i>5</i>
<i>Requisito 2: No utilice los valores predeterminados que ofrece el proveedor para las contraseñas del sistema u otros parámetros de seguridad.....</i>	<i>10</i>
Guía para los requisitos 3 y 4: Proteja los datos del titular de la tarjeta	13
<i>Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados</i>	<i>13</i>
<i>Requisito 4: Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.....</i>	<i>19</i>
Guía para los requisitos 5 y 6: Desarrolle un programa de administración de vulnerabilidad	21
<i>Requisito 5: Utilice y actualice regularmente el software o los programas antivirus</i>	<i>21</i>
<i>Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras</i>	<i>23</i>
Guía para los requisitos 7, 8 y 9: Implemente medidas sólidas de control de acceso	30
<i>Requisito 7: Restrinja el acceso a datos de titulares de tarjetas sólo a la necesidad de conocimiento de la empresa.....</i>	<i>30</i>
<i>Requisito 8: Asigne una ID única a cada persona que tenga acceso a computadoras.....</i>	<i>31</i>
<i>Requisito 9: Limite el acceso físico a los datos del titular de la tarjeta</i>	<i>35</i>
Guía para los requisitos 10 y 11: Supervise y pruebe las redes con regularidad.....	39
<i>Requisito 10: Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas.....</i>	<i>39</i>
<i>Requisito 11: Pruebe los sistemas y procesos de seguridad regularmente</i>	<i>42</i>
Guía para el requisito 12: Mantenga una política de seguridad de información.....	44
<i>Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas.....</i>	<i>44</i>
Guía para el requisito A.1: Requisitos de las PCI DSS adicionales para proveedores de hosting compartido.....	50
Anexo A: Normas de seguridad de datos de la PCI: documentos relacionados.....	52

Prefacio

Este documento describe los 12 requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), junto con orientación para explicar el propósito de cada requisito. Este documento pretende ayudar a comerciantes, proveedores de servicios e instituciones financieras que quizá deseen comprender las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago, y el significado específico y la intención detrás de los requisitos detallados para asegurar los componentes del sistema (servidores, redes, aplicaciones, etc.) que admiten entornos de datos de los titulares de las tarjetas.

NOTA: Exploración de PCI DSS: La comprensión del objetivo de los requisitos es sólo orientativa. Cuando se realiza un Cuestionario de Autoevaluación (SAQ) o una evaluación in situ de las PCI DSS, los requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad y los Cuestionarios de Autoevaluación de las PCI DSS, versión 1.2, son los documentos de registro.

Los requisitos de las PCI DSS se aplican a todos los componentes del sistema que se incluyen en el entorno de los datos del titular de la tarjeta o que están relacionados con éste. El entorno de los datos del titular de la tarjeta es la parte de la red que posee los datos del titular de la tarjeta o los datos confidenciales de autenticación, incluidos los componentes de la red, los servidores y las aplicaciones.

- Los componentes de la red incluyen, a modo de ejemplo, firewalls, interruptores, routers, puntos de acceso inalámbricos, dispositivos de red y otros dispositivos de seguridad.
- Los tipos de servidores incluyen, a modo de ejemplo: web, base de datos, autenticación, correo electrónico, proxy, protocolo de tiempo de red (NTP) y servidor de nombre de dominio (DNS).
- Las aplicaciones incluyen todas las aplicaciones compradas y personalizadas, incluidas las aplicaciones internas y externas (Internet).

La adecuada segmentación de red, que aísla los sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta de los que no lo hacen, puede reducir el alcance del entorno de los datos del titular. Un Asesor de Seguridad Certificado (QSA) puede ayudar a determinar el alcance dentro del entorno de los datos del titular de una entidad y brindar orientación sobre cómo reducir el alcance de una evaluación de las PCI DSS mediante la implementación de una segmentación de red adecuada. Si las empresas tienen preguntas acerca de si una implementación específica concuerda con la norma o si “cumple” con un requisito específico, las PCI SSC recomiendan que consulten con un Asesor de Seguridad Certificado (QSA) para validar su implementación de tecnología y procesos, y el cumplimiento de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago. La experiencia del QSA en el trabajo con entornos de red complejos se presta bien para ofrecer las mejores prácticas y orientación para el comerciante o proveedor de servicios que intenta lograr el cumplimiento. Puede encontrar la lista de PCI SSC de los Asesores de Seguridad Certificados en: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Elementos de los datos del titular de la tarjeta y de los datos confidenciales de autenticación

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

Los datos del titular de la tarjeta se definen como el número de cuenta principal (“PAN,” o número de tarjeta de crédito) y otros datos obtenidos como parte de una transacción de pago, incluidos los siguientes elementos de datos (para obtener información detallada vea debajo de la tabla).

- PAN
- Nombre del titular de la tarjeta
- Fecha de vencimiento
- Código de servicio
- Datos confidenciales de autenticación: (1) todos los datos de banda magnética, (2) CAV2/CVC2/CVV2/CID, y (3) los PIN/los bloqueos de PIN)

El número de cuenta principal (PAN) es el factor que define la aplicabilidad de los requisitos de las PCI DSS y las PA-DSS. Si no se almacena, procesa ni transmite el PAN, no se aplicarán las PCI DSS ni las PA-DSS.

	Elemento de datos	Almacenamiento permitido	Protección requerida	PCI DSS req. 3, 4
Datos del titular de la tarjeta	Número de cuenta principal	Sí	Sí	Sí
	Nombre del titular de la tarjeta ¹	Sí	Sí ¹	No
	Código de servicio ¹	Sí	Sí ¹	No
	Fecha de vencimiento ¹	Sí	Sí ¹	No
Datos confidenciales de autenticación ²	Datos completos de la banda magnética ³	No	N/C	N/C
	CAV2/CVC2/CVV2/CID	No	N/C	N/C
	PIN/Bloqueo de PIN	No	N/C	N/C

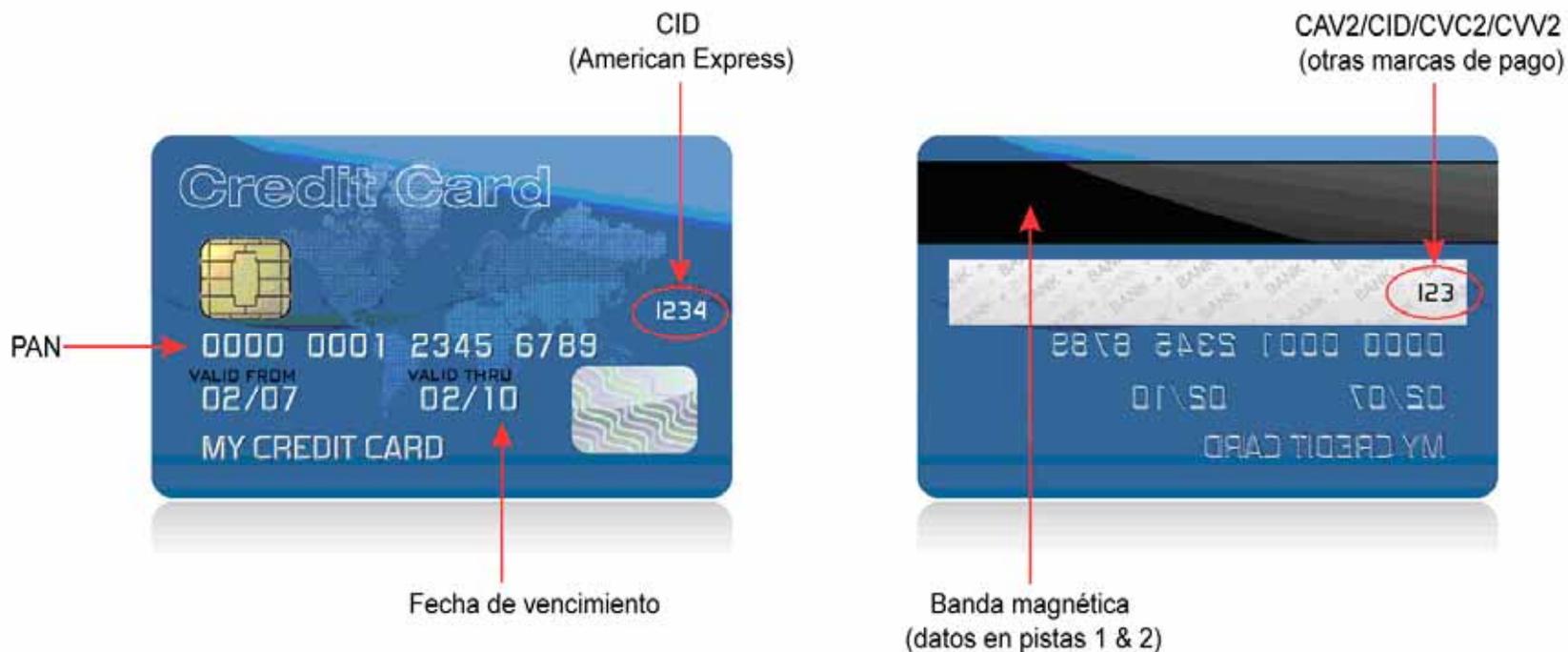
¹ Estos elementos de datos deben quedar protegidos si se los almacena con el PAN. Esta protección debe brindarse por cada requisito de las PCI DSS, a fin de asegurar una protección integral del entorno del titular de la tarjeta. Además, es posible que otras leyes (por ejemplo, las leyes relacionadas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

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

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

Ubicación de los datos de los titulares de tarjetas y de los datos confidenciales de autenticación

Los datos confidenciales de autenticación constan de datos⁴ de banda (o pista) magnética, el código de validación de la tarjeta o valor⁵ y los datos de PIN⁶. **¡Se prohíbe el almacenamiento de datos confidenciales de autenticación!** Estos datos son muy valiosos para las personas malintencionadas ya que les permiten generar tarjetas de pago falsas y crear transacciones fraudulentas. Consulte el *Glosario de términos, abreviaturas y acrónimos de las PCI DSS y las PA-DSS para obtener la definición completa de los “datos confidenciales de autenticación”*. Las imágenes del anverso y el reverso de la siguiente tarjeta de crédito muestran la ubicación del titular de la tarjeta y los datos confidenciales de autenticación.



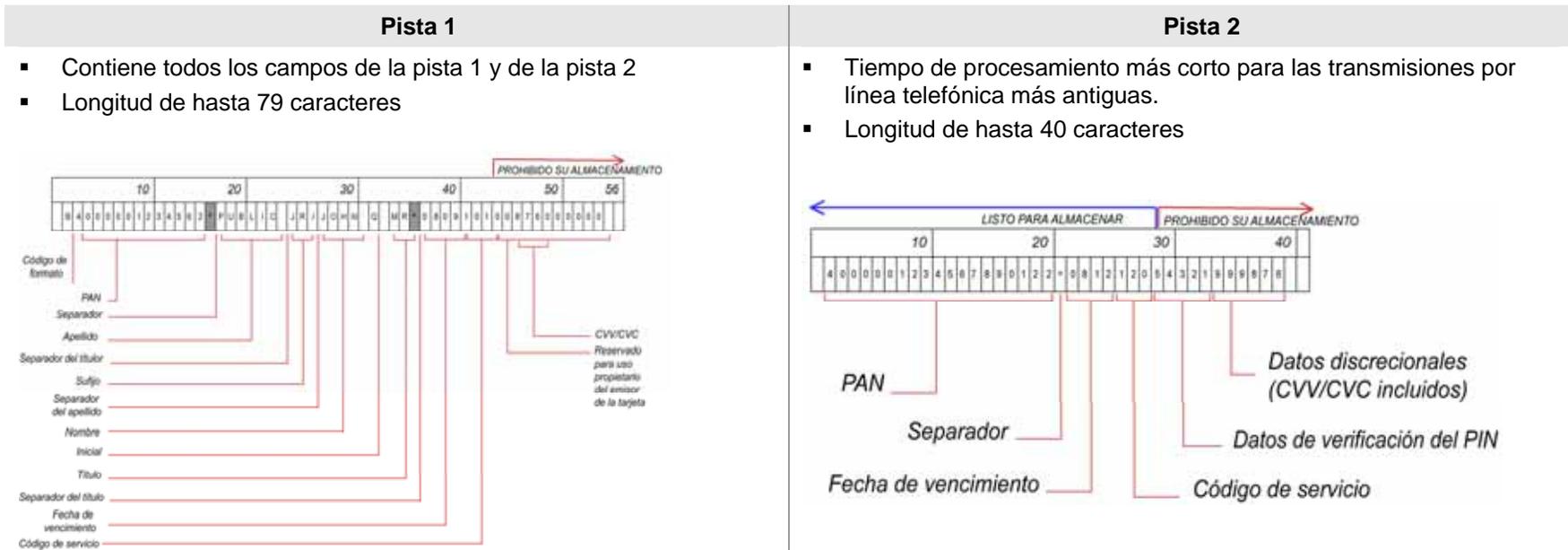
⁴ Datos codificados en la banda magnética que se utilizan para realizar la autorización durante una transacción con tarjeta presente. Estos datos también pueden encontrarse en la imagen de la banda magnética que está en el chip o en algún otro lugar de la tarjeta. Es posible que las entidades no retengan todos los datos de banda magnética después de la autorización de la transacción. Los únicos elementos de datos de pistas que se pueden retener son: el número de cuenta principal, el nombre del titular de la tarjeta, la fecha de vencimiento y el código de servicio.

⁵ El valor de tres o cuatro dígitos impreso en el panel de firma, a la derecha del panel de firma o en el anverso de la tarjeta de pago que se utiliza para verificar las transacciones con tarjeta ausente (CNP).

⁶ El número de identificación personal introducido por el titular de la tarjeta durante una transacción con tarjeta presente y/o el bloqueo del PIN cifrado presente dentro del mensaje de la transacción.

Datos de la pista 1 y pista 2

Si se almacena el contenido completo (ya sea de la pista 1 o de la pista 2 de banda magnética, imagen de la banda magnética que está en un chip o en cualquier otro dispositivo) las personas malintencionadas que obtienen datos pueden reproducir y vender tarjetas de pago en todo el mundo. El almacenamiento del contenido completo de la pista viola la reglamentación operativa de las marcas de pago y puede ocasionar multas o sanciones. La siguiente imagen ofrece información sobre los datos de la pista 1 y de la pista 2, mediante la descripción de las diferencias y la exhibición de la composición de los datos como están almacenados en la banda magnética.



Guía relacionada para las Normas de Seguridad de Datos de la PCI

Desarrollar y mantener una red segura

- Requisito 1: Instale y mantenga una configuración de firewall para proteger los datos de los titulares de las tarjetas
- Requisito 2: No utilice los valores predeterminados que ofrece el proveedor para las contraseñas del sistema u otros parámetros de seguridad.

Proteja los datos del titular de la tarjeta

- Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados
- Requisito 4: Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.

Desarrolle un programa de administración de vulnerabilidad

- Requisito 5: Utilice un software antivirus y actualícelo regularmente
- Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

Implemente medidas sólidas de control de acceso

- Requisito 7: Restrinja el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa
- Requisito 8: Asigne una ID única a cada persona que tenga acceso a computadoras
- Requisito 9: Limite el acceso físico a los datos del titular de la tarjeta

Supervise y pruebe las redes con regularidad

- Requisito 10: Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas
- Requisito 11: Pruebe los sistemas y procesos de seguridad regularmente

Mantenga una política de seguridad de información

- Requisito 12: Mantenga una política que aborde la seguridad de la información

Guía para los requisitos 1 y 2: Desarrollar y mantener una red segura

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

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

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

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

Requisito	Guía
1.1 Establezca las normas de configuración del firewall y del router que incluyen lo siguiente:	Los firewalls y los routers son componentes clave de la arquitectura que controlan la entrada a la red y la salida de ésta. Estos dispositivos son dispositivos de software o hardware que bloquean el acceso no deseado y administran el acceso autorizado de los elementos que entran y salen de la red. Sin la implementación de políticas y procedimientos para documentar cómo el personal debe configurar los firewalls y los routers, una empresa puede perder fácilmente su primera línea de defensa en la protección de datos. Las políticas y los procedimientos ayudarán a asegurar que la primera línea de defensa de la organización se mantenga fuerte en la protección de sus datos.
1.1.1 Un proceso formal para aprobar y evaluar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers	Una política y un proceso para aprobar y evaluar todas las conexiones y los cambios que se realizan en los firewalls y en los routers ayudarán a prevenir los problemas de seguridad que causa una mal configuración de la red, del router o del firewall.
1.1.2 Un diagrama actualizado de la red con todas las conexiones que acceden a los datos de los titulares de las tarjetas, incluida toda red inalámbrica	Los diagramas de red permiten a la organización identificar la ubicación de todos sus dispositivos de red. Además, el diagrama de red se puede usar para trazar el flujo de datos de los datos del titular de la tarjeta en la red y entre los dispositivos individuales para comprender plenamente el alcance del entorno del titular de la tarjeta. Sin diagramas de red y de flujos de datos actualizados, los dispositivos con datos del titular de la tarjeta pueden pasarse por alto e, inconscientemente, pueden dejarse afuera de los controles de seguridad en capas que se implementan para las PCI DSS y, por ende, tornarse vulnerables al peligro.

Requisito	Guía
<p>1.1.3 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier zona desmilitarizada (DMZ) y la zona de la red interna</p>	<p>El uso de un firewall en todas las conexiones que ingresan a la red (y las que salen) permite a la organización supervisar y controlar todo lo que entra y sale y minimizar las posibilidades de que personas malintencionadas logren obtener acceso a la red interna.</p>
<p>1.1.4 Descripción de grupos, de papeles y de responsabilidades para una administración lógica de los componentes de la red</p>	<p>Esta descripción de funciones y asignación de responsabilidades garantiza que alguien sea responsable de la seguridad de todos los componentes y que sea consciente de su responsabilidad, y que ningún dispositivo quede sin administrar.</p>
<p>1.1.5 Razón documentada y comercial para la utilización de todos los servicios, los protocolos y los puertos permitidos, incluida la documentación de funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros</p>	<p>Generalmente, los riesgos existen debido a servicios o puertos inseguros o que no se usan, ya que éstos generalmente tienen vulnerabilidades conocidas, y muchas organizaciones son vulnerables a estos tipos de riesgos porque no corrigen provisionalmente la vulnerabilidad de seguridad de los servicios, protocolos y puertos que no usan (aunque las vulnerabilidades aún estén presentes). Cada organización debe decidir de manera clara qué servicios, protocolos y puertos son necesarios para su empresa, documentarlos para sus registros y asegurarse de que todos los otros servicios, protocolos y puertos estén desactivados o se hayan eliminado. Además, las organizaciones deben considerar el bloqueo de todo el tránsito y sólo volver a abrir esos puertos una vez que se ha determinado y documentado una necesidad.</p> <p>Asimismo, existen muchos servicios, protocolos y puertos que una empresa puede necesitar (o ha activado de manera predeterminada) y que generalmente son usados por personas malintencionadas para poner en riesgo una red. Si estos servicios, protocolos y puertos inseguros son necesarios para la empresa, la organización debe comprender y aceptar el riesgo que ocasiona el uso de estos protocolos, se debe justificar el uso del protocolo y se deben documentar e implementar las funciones de seguridad que permiten que estos protocolos se usen de manera segura. Si estos servicios, protocolos y puertos inseguros no son necesarios para la empresa, deben desactivarse o eliminarse.</p>
<p>1.1.6 Requisitos de la revisión de las normas del firewall y del router, al menos, cada seis meses</p>	<p>Esta revisión le da una oportunidad a la organización, al menos cada seis meses, para limpiar toda norma innecesaria, obsoleta o incorrecta, y asegura que todas las normas permitan sólo servicios autorizados y puertos que se ajusten a razones comerciales.</p> <p>Se recomienda realizar estas revisiones con más frecuencia, por ejemplo, mensualmente, para garantizar que las normas estén actualizadas y satisfagan las necesidades de la empresa sin abrir los agujeros de seguridad y correr riesgos innecesarios.</p>

Requisito	Guía
<p>1.2 Desarrolle una configuración de firewall que restrinja las conexiones entre redes no confiables y todo componente del sistema en el entorno de los datos del titular de la tarjeta.</p> <p><i>Nota: Una "red no confiable" es toda red que es externa a las redes que pertenecen a la entidad en evaluación y que excede la capacidad de control o administración de la entidad.</i></p>	<p>Es esencial instalar protección de red, como un firewall, entre la red interna confiable y cualquier otra red no confiable externa o que excede la capacidad de control o administración de la entidad. Si no se implementa esta medida de manera correcta significa que la entidad será vulnerable al acceso no autorizado de personas malintencionadas y software malicioso.</p> <p>Si se instala un firewall pero no hay normas que controlen o limiten cierto tránsito, las personas malintencionadas aún pueden explotar los puertos y protocolos vulnerables para atacar su red.</p>
<p>1.2.1 Restrinja el tránsito entrante y saliente a la cantidad que sea necesaria en el entorno de datos del titular de la tarjeta.</p>	<p>Este requisito tiene como objetivo impedir que personas malintencionadas tengan acceso a la red de la organización a través de direcciones IP no autorizadas o a través del uso de servicios, protocolos o puertos de manera no autorizada (por ejemplo, para enviar a un servidor no confiable datos que han obtenido de su red).</p> <p>Todos los firewalls deben incluir una norma que niegue todo tránsito entrante y saliente que no sea específicamente necesario. Esto impide que haya agujeros inadvertidos que pueden permitir otro tránsito entrante o saliente accidental y potencialmente peligroso.</p>
<p>1.2.2 Asegure y sincronice los archivos de configuración de routers.</p>	<p>Si bien los archivos de configuración en ejecución generalmente se implementan con una configuración segura, es posible que los archivos de arranque (los routers sólo ejecutan estos archivos al reiniciarse) no se implementen con la misma configuración de seguridad porque sólo se ejecutan ocasionalmente. Cuando un router se reinicia sin la misma configuración segura que las de los archivos de configuración en ejecución, es posible que se produzcan normas más débiles que permitan que personas malintencionadas ingresen en la red, ya que es posible que los archivos de arranque no se hayan implementado con la misma configuración segura que los archivos de configuración en ejecución.</p>
<p>1.2.3 Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos firewalls para negar todo tránsito desde el entorno inalámbrico o para controlar (en caso de que ese tránsito fuera necesario para fines comerciales).</p>	<p>La implementación y explotación conocida (o desconocida) de tecnología inalámbrica dentro de una red es una vía común para que las personas malintencionadas obtengan acceso a la red y a los datos del titular de la tarjeta. Si se instala una red o un dispositivo inalámbrico sin que la empresa sepa, una persona malintencionada puede fácilmente e "inevitablemente" ingresar a la red. Si los firewalls no restringen el acceso desde redes inalámbricas hacia el entorno de la tarjeta de pago, las personas malintencionadas que obtienen acceso no autorizado a la red inalámbrica pueden conectarse fácilmente con el entorno de la tarjeta de pago y poner en riesgo la información de la cuenta.</p>

Requisito	Guía
<p>1.3 Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.</p>	<p>El propósito de un firewall es administrar y controlar todas las conexiones que hay entre sistemas públicos y sistemas internos (especialmente los que almacenan datos de titulares de tarjetas). Si se permite el acceso directo entre sistemas públicos y los que almacenan datos de titulares de tarjetas, se omite la protección que ofrece el firewall y los componentes del sistema que almacenan datos de titulares de tarjetas pueden estar en peligro.</p>
<p>1.3.1 Implemente un DMZ para limitar el tránsito entrante y saliente a los protocolos que sean necesarios en el entorno de datos del titular de la tarjeta.</p>	<p>Estos requisitos tienen como objetivo impedir que personas malintencionadas tengan acceso a la red de la organización a través de direcciones IP no autorizadas o a través del uso de servicios, protocolos o puertos de manera no autorizada (por ejemplo, para enviar a un servidor externo no confiable de una red no confiable datos que han obtenido de su red).</p>
<p>1.3.2 Restrinja el tránsito entrante de Internet a las direcciones IP dentro del DMZ.</p>	
<p>1.3.3 No permita ninguna ruta directa de entrada o salida de tránsito entre Internet y el entorno del titular de la tarjeta.</p>	<p>El DMZ es la parte del firewall que hace frente a la Internet pública y administra las conexiones entre Internet y los servicios internos que una organización necesita tener disponibles para el público (como un servidor web). Es la primera línea de defensa que aísla y separa el tránsito que necesita para comunicarse con la red interna del tráfico que no necesita comunicarse con la red interna.</p>
<p>1.3.4 No permita que las direcciones internas pasen desde Internet al DMZ.</p>	<p>Normalmente, un paquete contiene la dirección IP de la computadora que lo envió originalmente. Esto les permite a otras computadoras de la red saber de dónde viene ese paquete. En ciertos casos, personas malintencionadas falsificarán esta dirección IP.</p> <p>Por ejemplo, personas malintencionadas envían un paquete con una dirección falsa, de manera que (a menos que su firewall lo prohíba) el paquete ingresa a la red desde Internet, como tránsito interno y, por ende, legítimo. Una vez que las personas malintencionadas están dentro de la red, pueden poner en peligro sus sistemas.</p> <p>El filtrado de ingreso es una técnica que puede usar en su firewall para filtrar paquetes que ingresan en su red para, entre otras cosas, asegurarse de que los paquetes no se “falsifiquen” a fin de que parezca que provienen de su propia red interna.</p> <p>Si necesita más información sobre el filtrado de paquetes, puede obtener información sobre una técnica de consecuencia natural denominada “filtrado de salida”.</p>
<p>1.3.5 Restrinja el tránsito saliente del entorno de datos del titular de la tarjeta a Internet de forma tal que el tránsito saliente sólo pueda acceder a direcciones IP dentro del DMZ.</p>	<p>El DMZ también debe evaluar todo el tránsito saliente desde el interior de la red para asegurar que todo el tránsito saliente siga las normas establecidas. Para que el DMZ realice esta función con eficacia, no se deben permitir conexiones desde el interior de la red hacia cualquier dirección fuera de la red, a menos que antes pasen por el DMZ y este evalúe su legitimidad.</p>

Requisito	Guía
<p>1.3.6 Implemente la inspección completa, también conocida como filtrado dinámico de paquetes. (Es decir, sólo se permite la entrada a la red de conexiones “establecidas”).</p>	<p>Un firewall que realiza una inspección meticulosa de paquetes mantiene el “estado” (o el estatus) de todas las conexiones del firewall. Al mantener el “estado”, el firewall sabe si lo que parece ser una respuesta a una conexión anterior es verdaderamente una respuesta (ya que “recuerda” la conexión anterior) o es un software malicioso o una persona malintencionada que intenta burlar o engañar el firewall para que permita la conexión.</p>
<p>1.3.7 Coloque la base de datos en una zona de red interna, segregada del DMZ.</p>	<p>Los datos del titular de la tarjeta requieren el mayor nivel de protección de la información. Si se ubican datos del titular de la tarjeta dentro del DMZ, el acceso a esta información es más simple para un atacante externo, ya que hay menos capas para penetrar.</p>
<p>1.3.8 Implemente la simulación IP a los efectos de evitar que las direcciones internas se traduzcan y se divulguen en Internet mediante la utilización del espacio de dirección RFC 1918. Utilice tecnologías de traducción de dirección de red (NAT), por ejemplo, traducción de dirección de puertos (PAT).</p>	<p>La simulación IP, que administra el firewall, permite a una organización tener direcciones internas que son sólo visibles dentro de la red y direcciones externas que son visibles fuera de la red. Si un firewall no “esconde” u oculta las direcciones IP de la red interna, una persona malintencionada puede descubrir direcciones IP internas e intentar acceder a la red con una dirección IP falsa.</p>
<p>1.4 Instale software de firewall personal en toda computadora móvil o de propiedad de los trabajadores con conectividad directa a Internet (por ejemplo, laptops que usan los trabajadores), mediante las cuales se accede a la red de la organización.</p>	<p>Si una computadora no tiene un firewall o un programa antivirus instalado, se pueden descargar spyware, troyanos, virus, gusanos y rootkit (malware) o instalarse sin saberlo. La computadora es aún más vulnerable cuando está directamente conectada a Internet y no detrás del firewall de la empresa. El malware cargado en una computadora que no está protegida por el firewall de la empresa puede dirigirse maliciosamente a la información que hay en la red cuando la computadora se vuelve a conectar a la red corporativa.</p>

Requisito 2: No utilice los valores predeterminados que ofrece el proveedor para las contraseñas del sistema u otros parámetros de seguridad.

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

Requisito	Guía
<p>2.1 Siempre cambie los valores predeterminados de los proveedores antes de instalar un sistema en la red (por ejemplo, incluya contraseñas, cadenas comunitarias de protocolo simple de administración de red [SNMP] y elimine cuentas innecesarias).</p>	<p>Los delincuentes (externos e internos a la empresa), por lo general, utilizan las contraseñas, los nombres de cuenta y los valores de configuración predeterminados por los proveedores para afectar los sistemas. Las comunidades de hackers conocen bien estos valores de configuración y hacen que su sistema sea muy vulnerable a un ataque.</p>
<p>2.1.1 En el caso de entornos inalámbricos que están conectados al entorno de datos del titular de la tarjeta o que transfieren datos del titular de la tarjeta, cambie los valores predeterminados proporcionados por los proveedores, incluidas, a modo de ejemplo, claves de criptografía inalámbricas predeterminadas, contraseñas y cadenas comunitarias SNMP. Asegúrese de que la configuración de seguridad de los dispositivos inalámbricos esté habilitada para la tecnología de cifrado de la autenticación y transmisión.</p>	<p>Muchos usuarios instalan estos dispositivos sin la aprobación de la gerencia y no cambian los valores de configuración predeterminados ni establecen la configuración de seguridad. Si las redes inalámbricas no se implementan con suficientes configuraciones de seguridad (incluido el cambio de los valores de configuración predeterminados), los analizadores inalámbricos de protocolos pueden espiar el tránsito, capturar datos y contraseñas de manera sencilla e ingresar fácilmente en su red y atacarla. Además, se ha roto el protocolo de intercambio clave para la versión anterior de cifrado 802.11x (WEP) y puede hacer que el cifrado sea inútil. Verifique que el firmware de los dispositivos esté actualizado para admitir protocolos más seguros, como WPA/WPA2.</p>

Requisito	Guía
<p>2.2 Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria.</p>	<p>Existen debilidades conocidas en muchos sistemas operativos, bases de datos y aplicaciones de empresas, y también existen formas conocidas de configurar estos sistemas para arreglar las vulnerabilidades de seguridad. Para ayudar a quienes no son expertos en seguridad, las organizaciones de seguridad han establecido recomendaciones de alta seguridad de sistema, que aconsejan cómo corregir estas debilidades. Si no se eliminan estas debilidades de los sistemas, como una configuración de archivo débil o servicios y protocolos predeterminados (para los servicios o protocolos que generalmente no son necesarios), un atacante puede usar distintos puntos vulnerables conocidos para atacar servicios y protocolos vulnerables y, así, obtener acceso a la red de la organización. Puede visitar estos tres sitios web de ejemplo, en los que podrá obtener más información sobre las mejores prácticas de la industria que pueden ayudarlo a implementar normas de configuración: www.nist.gov, www.sans.org, www.cisecurity.org.</p>
<p>2.2.1 Implemente solamente una función principal por cada servidor.</p>	<p>Esto tiene como objetivo garantizar que las normas de configuración de los sistemas y los procesos relacionados de una empresa tratan las funciones de los servidores que necesitan tener distintos niveles de seguridad o que pueden introducir debilidades de seguridad en otras funciones del mismo servidor. Por ejemplo:</p> <ol style="list-style-type: none"> 1. Una base de datos, que requiere fuertes medidas de seguridad, estaría en riesgo si compartiera un servidor con una aplicación web, que necesita estar abierta y enfrenarse directamente con Internet. 2. Si no se aplica un parche a una función aparentemente menor se puede correr un riesgo que puede repercutir en otras funciones más importantes (como la base de datos) del mismo servidor. <p>Este requisito es para servidores (generalmente Unix, Linux o Windows), pero no para sistemas mainframe.</p>
<p>2.2.2 Deshabilite todos los servicios y protocolos innecesarios e inseguros (servicios y protocolos que no sean directamente necesarios para desempeñar la función especificada de los dispositivos).</p>	<p>Como se mencionó en 1.1.7, existen muchos protocolos que una empresa puede necesitar (o ha activado de manera predeterminada) y que generalmente son usados por personas malintencionadas para poner en riesgo una red. Para garantizar que estos servicios y protocolos estén siempre desactivados cuando se implementan nuevos servidores, este requisito debe ser parte de las normas de configuración y los procesos relacionados de su empresa.</p>

Requisito	Guía
<p>2.2.3 Configure los parámetros de seguridad del sistema para evitar el uso indebido.</p>	<p>Esto pretende garantizar que las normas de configuración de los sistemas y los procesos relacionados de su empresa traten específicamente los parámetros y la configuración de seguridad que han conocido implicaciones de seguridad.</p>
<p>2.2.4 Elimine todas las funcionalidades innecesarias, tales como secuencias de comandos, controladores, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.</p>	<p>Las normas de alta seguridad de servidor deben incluir procesos para abordar las funcionalidades innecesarias con implicaciones de seguridad específicas (como eliminar/desactivar el FTP o el servidor web si el servidor no ejecutará esas funciones).</p>
<p>2.3 Cifre el acceso administrativo que no sea de consola. Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y otros tipos de acceso administrativo que no sea de consola.</p>	<p>Si la administración remota no se realiza con autenticación segura y comunicaciones cifradas, la información confidencial de nivel operativo o administrativo (como las contraseñas de los administradores) puede revelarse a un espía. Una persona malintencionada puede usar esta información para acceder a la red, convertirse en administrador y robar datos.</p>
<p>2.4 Los proveedores de servicio de hosting deben proteger el entorno hosting y los datos del titular de la tarjeta. Estos proveedores deben cumplir requisitos específicos detallados en el <i>“Anexo A: Requisitos de las PCI DSS adicionales para proveedores de hosting compartido”</i>.</p>	<p>Este punto está pensado para los proveedores de hosting que ofrecen entornos de servicio de hosting compartido para varios clientes en el mismo servidor. En general, cuando todos los datos están en el mismo servidor, bajo el control de un solo entorno, los clientes individuales no pueden controlar la configuración de estos servidores, pero se les permite agregar secuencias y funciones inseguras que afectan la seguridad de los entornos de los otros clientes y, por ende, hacen que sea más fácil para las personas malintencionadas poner en riesgo los datos de un cliente y, así, obtener acceso a todos los otros datos de los clientes. Consulte el Anexo A.</p>

Guía para los requisitos 3 y 4: Proteja los datos del titular de la tarjeta

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

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

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

Requisito	Guía
<p>3.1 Almacene la menor cantidad de datos posibles del titular de la tarjeta. Desarrolle una política de retención y de disposición de datos. Reduzca la cantidad de datos almacenados y el tiempo de retención a los que sean necesarios para fines comerciales, legales o reglamentarios, según se documente en la política de retención de datos.</p>	<p>El almacenamiento de gran extensión de datos de los titulares de las tarjetas que excede la necesidad de la empresa crea un riesgo innecesario. Los únicos datos de los titulares de las tarjetas que pueden almacenarse son el número de cuenta principal o PAN (ilegible), la fecha de vencimiento, el nombre y el código de servicio. Recuerde: si no lo necesita, ¡no lo almacene!</p>
<p>3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3 establecidos a continuación.</p>	<p>Los datos confidenciales de autenticación constan de datos⁷ de banda (o pista) magnética, el código de validación de la tarjeta o valor⁸ y los datos de PIN⁹. ¡Se prohíbe el almacenamiento de datos confidenciales de autenticación después de recibir la autorización! Estos datos son muy valiosos para las personas malintencionadas ya que les permiten generar tarjetas de pago falsas y crear transacciones fraudulentas. Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS y las PA-DSS para obtener la definición completa de los "datos confidenciales de autenticación".</p>

⁷ Datos codificados en la banda magnética que se utilizan para realizar la autorización durante una transacción con tarjeta presente. Estos datos también pueden encontrarse en la imagen de la banda magnética que está en el chip o en algún otro lugar de la tarjeta. Es posible que las entidades no retengan todos los datos de banda magnética después de la autorización de la transacción. Los únicos elementos de datos de pistas que se pueden retener son: el número de cuenta principal, el nombre del titular de la tarjeta, la fecha de vencimiento y el código de servicio.

⁸ El valor de tres o cuatro dígitos impreso en el panel de firma, a la derecha del panel de firma o en el anverso de la tarjeta de pago que se utiliza para verificar las transacciones con tarjeta ausente (CNP).

⁹ El número de identificación personal introducido por el titular de la tarjeta durante una transacción con tarjeta presente y/o el bloqueo del PIN cifrado presente dentro del mensaje de la transacción.

Requisito	Guía
<p>3.2.1 No almacene contenidos completos de ninguna pista de la banda magnética (que está en el reverso de la tarjeta, en un chip o en cualquier otro dispositivo). Estos datos se denominan alternativamente, pista completa, pista, pista 1, pista 2 y datos de banda magnética.</p> <p><i>Nota: En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:</i></p> <ul style="list-style-type: none"> ▪ El nombre del titular de la tarjeta. ▪ Número de cuenta principal (PAN). ▪ Fecha de vencimiento. ▪ Código de servicio. <p><i>Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.</i></p> <p><i>Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información.</i></p>	<p>Si se almacena el contenido completo, las personas malintencionadas que obtienen datos pueden reproducir y vender tarjetas de pago en todo el mundo.</p>
<p>3.2.2 No almacene el valor ni el código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago) que se utiliza para verificar las transacciones de tarjetas ausentes.</p> <p><i>Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información.</i></p>	<p>El objetivo del código de validación de la tarjeta es proteger las transacciones de “tarjetas ausentes” (transacciones de pedidos por Internet o correo/ teléfono). Estos tipos de transacciones pueden autenticarse y demostrar que provienen del propietario de la tarjeta con sólo solicitar este código de validación de la tarjeta, ya que el propietario tiene la tarjeta en la mano y puede leer el valor. Si estos datos prohibidos se almacenan y luego son robados, las personas malintencionadas pueden ejecutar transacciones de pedidos por Internet o correo/teléfono fraudulentas.</p>
<p>3.2.3 No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.</p>	<p>Sólo el propietario de la tarjeta o el banco que la emitió deben conocer estos valores. Si estos datos prohibidos se almacenan y luego son robados, las personas malintencionadas pueden ejecutar transacciones de débito con PIN fraudulentas.</p>

Requisito	Guía
<p>3.3 Oculte el PAN cuando aparezca (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá).</p> <p><i>Notas:</i></p> <ul style="list-style-type: none"> ▪ <i>Este requisito no se aplica a trabajadores y a otras partes que posean una necesidad específica de conocer el PAN completo.</i> ▪ <i>Este requisito no reemplaza los requisitos más estrictos que fueron implementados y que aparecen en los datos del titular de la tarjeta (por ejemplo, los recibos de puntos de venta [POS]).</i> 	<p>La aparición del PAN completo en artículos como las pantallas de computadoras, los recibos de tarjetas de pago, los faxes o los informes en papel puede facilitar la obtención de estos datos por parte de individuos no autorizados y su uso fraudulento. El PAN puede mostrarse completo en los recibos de “copia de comerciantes”; sin embargo, los recibos en papel deben adherirse a los mismos requisitos de seguridad que las copias electrónicas y seguir los lineamientos de las Normas de Seguridad de Datos de la PCI, especialmente el Requisito 9 sobre seguridad física. El PAN completo también puede mostrarse a quienes tienen una necesidad comercial legítima de visualizar el PAN completo.</p>
<p>3.4 Haga que el PAN quede, como mínimo, ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles y en registros) utilizando cualquiera de los siguientes métodos:</p> <ul style="list-style-type: none"> ▪ Valores hash de una vía en criptografía sólida ▪ Truncamiento. ▪ Token y ensambladores de índices (los ensambladores se deben almacenar de manera segura). 	<p>La falta de protección del PAN puede permitir a los individuos malintencionados visualizar o descargar estos datos. Todos los PAN que se almacenan en almacenamiento principal (bases de datos o archivos planos, como hojas de cálculo de archivos de texto) y en almacenamiento no principal (copias de seguridad, registros de auditoría, registros de excepción o resolución de problemas) deben protegerse. El daño ocasionado por el robo o la pérdida de cintas de respaldo durante el transporte puede reducirse si se asegura que los PAN sean ilegibles mediante el cifrado, el truncamiento y la refundición. Como los registros de auditoría, de resolución de problemas y de excepción deben conservarse, puede impedir la divulgación de los datos del registro si se asegura que los PAN sean ilegibles (los elimina u oculta) en los registros. Consulte el <i>Glosario de términos, abreviaturas y acrónimos de las PCI DSS y las PA-DSS</i> para obtener definiciones de “criptografía sólida”.</p> <p>Los valores hash de una vía (como SHA-1) en criptografía sólida pueden usarse para que los datos de los titulares de tarjetas sean ilegibles. Los valores hash son apropiados cuando no hay necesidad de recuperar el número original (los valores hash de una vía son irreversibles).</p> <p>El propósito del truncamiento es que se almacene sólo una porción del PAN (que no se superen los primeros seis dígitos y los últimos cuatro). Esto es distinto al ocultamiento, en donde el PAN completo se almacena pero se oculta cuando aparece (es decir, sólo aparece una parte del PAN en las pantallas, los informes, los recibos, etc.).</p> <p>Los tokens y ensambladores de índices también pueden usarse para que los datos de los titulares de tarjetas sean ilegibles. Un token de índice es un token criptográfico que reemplaza el PAN en base a un índice dado para un valor imprevisible. Un ensamblador de una vez es un sistema en el que una clave privada, que se genera de forma aleatoria, se usa sólo una vez para cifrar un mensaje que luego se descifra con un ensamblador de una vez y una clave.</p>

Requisito	Guía
<ul style="list-style-type: none"> ▪ Criptografía sólida con procesos y procedimientos de gestión de claves relacionadas. <p><i>La información de cuenta MÍNIMA que se debe dejar ilegible es el PAN.</i></p> <p>Notas:</p> <ul style="list-style-type: none"> ▪ <i>Si por alguna razón, la empresa no puede hacer que el PAN sea ilegible, consulte el “Anexo B: Controles de compensación”.</i> ▪ La “criptografía sólida” se define en el Glosario de términos, abreviaturas y acrónimos de las PCI DSS. 	<p>El propósito de una criptografía sólida (consulte la definición y las longitudes de las claves en el <i>Glosario de términos, abreviaturas y acrónimos de las PCI DSS</i>) es que el cifrado esté basado en un algoritmo probado y aceptado en la industria (no en un algoritmo propietario o propio).</p>
<p>3.4.1 Si se utiliza cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independientemente de los mecanismos de control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales). Las claves de descifrado no deben estar vinculadas a cuentas de usuarios.</p>	<p>El objetivo de este requisito es tratar la aceptabilidad del cifrado de disco para que los datos de los titulares de tarjetas sean ilegibles. El cifrado de disco cifra los datos almacenados en el almacenamiento masivo de una computadora y descifra automáticamente la información cuando un usuario autorizado la solicita. Los sistemas de cifrado de disco interceptan las operaciones de lectura y escritura del sistema operativo y realizan las transformaciones criptográficas apropiadas sin ninguna acción especial por parte del usuario; sólo debe suministrar una contraseña o frase al iniciar sesión. En base a estas características de cifrado de disco, para cumplir con este requisito, el método de cifrado de disco no puede tener:</p> <ol style="list-style-type: none"> 1) Una asociación directa con el sistema operativo. 2) Claves de descifrado asociadas con las cuentas de usuario.
<p>3.5 Proteja las claves criptográficas que se utilizan para cifrar los datos de los titulares de tarjetas contra su posible divulgación o uso indebido:</p>	<p>Las claves criptográficas deben estar muy protegidas porque quienes obtienen acceso podrán descifrar los datos.</p>
<p>3.5.1 Restrinja el acceso a las claves criptográficas al número mínimo de custodios necesarios.</p>	<p>Muy pocas personas deben tener acceso a claves criptográficas; generalmente, sólo quienes tienen responsabilidad como custodios de las claves.</p>
<p>3.5.2 Guarde las claves criptográficas de forma segura en la menor cantidad de ubicaciones y formas posibles.</p>	<p>Las claves criptográficas deben almacenarse de manera segura, generalmente con claves de cifrado, y en muy pocos lugares.</p>

Requisito	Guía
3.6 Documento completamente e implemente todos los procesos y los procedimientos de gestión de claves de las claves criptográficas que se utilizan para el cifrado de datos de titulares de tarjetas, incluido lo siguiente:	La forma en la que se gestionan las claves criptográficas es una parte fundamental de la seguridad constante de la solución de cifrado. Un buen procedimiento de gestión de claves, ya sea manual o automático como parte del producto de cifrado, incluye todos los elementos clave desde 3.6.1 hasta 3.6.8.
3.6.1 Generación de claves criptográficas sólidas	La solución de cifrado debe generar claves sólidas, según se define en el <i>Glosario de términos, abreviaturas y acrónimos de las PCI DSS</i> en “criptografía sólida”.
3.6.2 Distribución segura de claves criptográficas	La solución de cifrado debe distribuir las claves de manera segura; esto significa que las claves no se distribuyen en el espacio libre y que sólo son distribuidas a los custodios que se identifican en 3.5.1.
3.6.3 Almacenamiento seguro de claves criptográficas	La solución de cifrado debe almacenar las claves de manera segura; esto significa que las claves no se almacenan en el espacio libre (cifrelas con una clave de cifrado de clave).
3.6.4 Cambios periódicos de claves criptográficas <ul style="list-style-type: none"> • Según se considere necesario y lo recomiende la aplicación asociada (por ejemplo, volver a digitar las claves), preferentemente en forma automática • Por lo menos, anualmente 	Si el proveedor de aplicación de cifrado le suministra recomendaciones o procesos del proveedor para el cambio periódico de claves, sígalos. El cambio anual de claves de cifrado es imprescindible para minimizar el riesgo de que alguien obtenga las claves de cifrado y pueda descifrar los datos.
3.6.5 Destrucción o reemplazo de claves criptográficas antiguas o supuestamente en riesgo	Las claves antiguas que ya no se usan ni se necesitan deben retirarse o destruirse para asegurarse de que no se vuelvan a usar. Si es necesario conservar las claves antiguas (por ejemplo, para respaldar los datos cifrados y archivados), debe protegerlas muy bien (consulte 3.6.6 a continuación). La solución de cifrado también debe permitir y facilitar un proceso para reemplazar claves que sepa que están sospechadas o en riesgo.
3.6.6 Divida el conocimiento y la creación del control dual de claves criptográficas	La división del conocimiento y el control dual de claves se usan para eliminar la posibilidad de que una persona tenga acceso a toda la clave. Generalmente, este control se aplica en sistemas de cifrado de clave manuales o donde el producto de cifrado no implementa la gestión de claves. Por lo general, este tipo de control se implementa dentro de módulos de seguridad de hardware.

Requisito	Guía
3.6.7 Prevención de sustitución no autorizada de claves criptográficas	La solución de cifrado no debe permitir ni aceptar la sustitución de claves provenientes de fuentes no autorizadas ni procesos inesperados.
3.6.8 Requisito de que los custodios de claves criptográficas firmen un formulario en el que declaren que comprenden y aceptan su responsabilidad como custodios de las claves	Este proceso garantiza que el individuo se compromete con el rol de custodio de las claves y comprende sus responsabilidades.

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

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

Requisito	Guía
<p>4.1 Utilice criptografía y protocolos de seguridad sólidos como SSL/TLS o IPSEC para salvaguardar los datos confidenciales de los titulares de las tarjetas durante su transmisión a través de redes públicas abiertas.</p> <p><i>Ejemplos de redes públicas abiertas que se encuentran dentro del alcance de las DSS de la PCI son:</i></p> <ul style="list-style-type: none"> ▪ Internet ▪ Tecnologías inalámbricas ▪ Sistema global de comunicaciones móviles (GSM) ▪ Servicio de radio paquete general (GPRS) 	<p>La información confidencial se debe codificar durante su transmisión a través de redes públicas, ya que para una persona malintencionada es simple y común interceptar o desviar datos mientras se transmiten. La Capa de Conexión Segura (SSL) cifra páginas web y los datos que se ingresan en éstas. Cuando use sitios web asegurados con SSL, asegúrese de que “https” esté en el URL.</p> <p>Tenga en cuenta que las versiones de SSL anteriores a v3.0 contienen vulnerabilidades documentadas, como desbordamientos de buffer, que un atacante puede usar para obtener el control del sistema afectado.</p>

Requisito	Guía
<p>4.1.1 Asegúrese de que las redes inalámbricas que transmiten datos de los titulares de las tarjetas o que están conectadas al entorno de datos del titular de la tarjeta utilizan las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) a los efectos de implementar cifrados sólidos para la autenticación y transmisión.</p> <ul style="list-style-type: none"> ▪ <i>En el caso de nuevas implementaciones inalámbricas, se prohíbe la implementación WEP después del 31 de marzo de 2009.</i> ▪ <i>En el caso de actuales implementaciones inalámbricas, se prohíbe la implementación WEP después del 30 de junio de 2010.</i> 	<p>Los usuarios malintencionados usan herramientas gratuitas y ampliamente disponibles para espiar las comunicaciones inalámbricas. El uso del cifrado apropiado puede impedir que estos individuos espíen y divulguen información confidencial en la red. Muchos riesgos conocidos de datos de titulares de tarjetas almacenados sólo en la red cableada se originan cuando un usuario malintencionado extiende el acceso de una red inalámbrica insegura.</p> <p>Se necesita un cifrado sólido para la autenticación y transmisión de los datos de titulares de tarjetas para poder impedir que usuarios malintencionados obtengan acceso a la red inalámbrica (a los datos de la red) o utilicen las redes inalámbricas para tener acceso a otras redes inalámbricas o datos. WEP no utiliza un cifrado sólido. El cifrado WEP nunca debe usarse solo, ya que es vulnerable debido a vectores iniciales débiles (IV) en el proceso de intercambio de clave WEP, y la falta de la rotación de claves necesaria. Un atacante puede usar herramientas de craqueo de fuerza bruta para penetrar el cifrado WEP.</p> <p>Los dispositivos inalámbricos actuales deben actualizarse (por ejemplo: actualizar el firmware de punto de acceso a WPA) para admitir un cifrado sólido. Si los dispositivos actuales no pueden actualizarse, es necesario adquirir nuevas computadoras.</p> <p>Si las redes inalámbricas están usando WEP, no deben tener acceso a entornos de datos de los titulares de las tarjetas.</p>
<p>4.2 Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea o el chat).</p>	<p>El correo electrónico, la mensajería instantánea y el chat pueden ser fácilmente interceptados por el olfateo de paquetes durante la entrega en redes internas y públicas. No utilice estas herramientas de mensajería para enviar PAN a menos que le ofrezcan capacidades de cifrado.</p>

Guía para los requisitos 5 y 6: Desarrolle un programa de administración de vulnerabilidad

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

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

Requisito	Guía
<p>5.1 Implemente software antivirus en todos los sistemas comúnmente afectados por software malicioso (en especial, computadoras personales y servidores).</p>	<p>Hay un flujo constante de ataques que usan puntos vulnerables ampliamente publicados, generalmente "día cero" (publicado y extendido en las redes no más de una hora después de su descubrimiento) contra sistemas que no están asegurados. Sin un software antivirus que se actualice regularmente, estas nuevas formas de software malicioso pueden atacar y desactivar su red.</p> <p>El software malicioso puede descargarse sin saberlo o instalarse de Internet, pero las computadoras también son vulnerables cuando se usan dispositivos de almacenamiento extraíbles, como CD y DVD, memorias USB y discos duros, cámaras digitales, asistentes digitales personales (PDA) y otros dispositivos periféricos. Si estas computadoras no tienen ningún software antivirus instalado, pueden convertirse en puntos de acceso a su red y dirigirse maliciosamente a la información que hay en la red.</p> <p>Si bien los sistemas que comúnmente se ven afectados por software malicioso, en general, no incluyen mainframes y la mayoría de los sistemas Unix (consulte más detalles a continuación), cada entidad debe tener un proceso según el Requisito 6.2 de las PCI DSS para identificar y tratar las nuevas vulnerabilidades de seguridad y actualizar sus procesos y normas de configuración. Las tendencias en software malicioso relacionadas con los sistemas operativos que usa una entidad deben incluirse en la identificación de las nuevas vulnerabilidades de seguridad y los métodos para tratar nuevas tendencias deben incorporarse en las normas de configuración y los mecanismos de protección de la empresa según sea necesario.</p> <p>Generalmente, el software malicioso no afecta estos sistemas operativos: mainframes y ciertos servidores Unix (como AIX, Solaris y HP-Unix). Sin embargo, las tendencias de la industria para software malicioso pueden cambiar rápidamente y cada organización debe cumplir con el Requisito 6.2 para identificar y tratar las nuevas vulnerabilidades de seguridad y actualizar sus procesos y normas de configuración.</p>

Requisito	Guía
5.1.1 Asegúrese de que todos los programas antivirus sean capaces de detectar y eliminar todos los tipos conocidos de software malicioso y de proteger los sistemas contra estos.	Es importante proteger las computadoras contra TODO tipo y forma de software malicioso.
5.2 Asegúrese de que todos los mecanismos antivirus son actuales, están en funcionamiento y son capaces de generar registros de auditoría.	El mejor software antivirus es limitado en eficacia si no tiene las firmas antivirus actualizadas o si no está activa en la red o en una computadora. Los registros de auditoría ofrecen la capacidad de supervisar la actividad de los virus y las reacciones antivirus.

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

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

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

Requisito	Guía
<p>6.1 Asegúrese de que todos los componentes de sistemas y software cuenten con los parches de seguridad más recientes proporcionados por los proveedores. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento.</p> <p><i>Nota: Las organizaciones pueden tener en cuenta la aplicación de un enfoque basado en el riesgo a los efectos de priorizar la instalación de parches. Por ejemplo, al priorizar infraestructura de importancia (por ejemplo, dispositivos y sistemas públicos, bases de datos) superiores a los dispositivos internos menos críticos a los efectos de asegurar que los dispositivos y los sistemas de alta prioridad se traten dentro del periodo de un mes y se traten dispositivos y sistemas menos críticos dentro de un periodo de tres meses.</i></p>	<p>Existe una gran cantidad de ataques que usan puntos vulnerables ampliamente publicados, generalmente "día cero" (publicado y extendido en una hora) contra los sistemas que no están asegurados. Si no se implementan los parches más recientes en los sistemas importantes lo antes posible, una persona malintencionada puede usar estos puntos vulnerables para atacar y desactivar la red. Considere priorizar cambios como los parches importantes de seguridad para los sistemas importantes o en riesgo que pueden instalarse en no más de 30 días y otros cambios menos riesgosos que pueden instalarse en no más de 2 ó 3 meses.</p>
<p>6.2 Establezca un proceso para identificar las vulnerabilidades de seguridad recientemente descubiertas (por ejemplo, suscríbase a los servicios de alerta disponibles de forma gratuita a través de Internet). Actualice las normas de configuración conforme al Requisito 2.2 de las DSS de la PCI para subsanar cualquier otro problema de vulnerabilidad.</p>	<p>El objetivo de este requisito es que las organizaciones se mantengan actualizadas con respecto a las nuevas vulnerabilidades para que puedan proteger de manera apropiada su red e incorporar las vulnerabilidades recientemente descubiertas y relevantes en sus normas de configuración.</p>

Requisito	Guía
<p>6.3 Desarrolle aplicaciones de software conforme a las DSS de la PCI (por ejemplo, registro y autenticación seguros) sobre la base de las mejores prácticas de la industria e incorpore la seguridad de la información en todo el ciclo de desarrollo de software. Los procesos deben incluir lo siguiente:</p>	<p>Sin la inclusión de seguridad durante las fases de desarrollo de software de definición de requisitos, diseño, análisis y prueba, las vulnerabilidades de seguridad pueden introducirse de forma inadvertida o maliciosamente en el entorno de producción.</p>
<p>6.3.1 La prueba de todos los parches de seguridad y los cambios de configuración del sistema y del software antes de su implementación</p> <p>6.3.1.1 Validación de las entradas (para prevenir el lenguaje de comandos entre distintos sitios, los errores de inyección, la ejecución de archivos maliciosos, etc.)</p> <p>6.3.1.2 Validación de un correcto manejo de los errores</p> <p>6.3.1.3 Validación del almacenamiento criptográfico seguro.</p> <p>6.3.1.4 Validación de las comunicaciones seguras</p> <p>6.3.1.5 Validación de un correcto control del acceso basado en funciones (RBAC)</p>	<p>Asegúrese de que todas las instalaciones y los cambios se realicen de la manera esperada y que no tengan ninguna función inesperada, no deseada o dañina.</p>
<p>6.3.2 Desarrollo/prueba por separado y entornos de producción</p>	<p>Generalmente, los entornos de desarrollo y prueba son menos seguros que el entorno de producción. Sin una separación adecuada, el entorno de producción y los datos de titulares de tarjetas pueden estar en riesgo debido a vulnerabilidades o procesos internos débiles.</p>
<p>6.3.3 Separación de funciones entre desarrollo/prueba y entornos de producción</p>	<p>Esto minimiza la cantidad de personal con acceso al entorno de producción y a los datos de titulares de tarjetas y ayuda a garantizar que el acceso quede limitado a quienes verdaderamente necesitan ese acceso.</p>
<p>6.3.4 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo</p>	<p>En general, los controles de seguridad no son tan estrictos en el entorno de desarrollo. El uso de datos de producción ofrece a las personas malintencionadas la posibilidad de obtener acceso no autorizado a datos de producción (datos de titulares de tarjetas).</p>

Requisito	Guía
<p>6.3.5 Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción</p>	<p>Los datos y las cuentas de prueba se deben eliminar del código de producción antes de que se active la aplicación, ya que estos elementos pueden revelar información sobre el funcionamiento de la aplicación. La posesión de esta información puede poner en riesgo la aplicación y los datos de titulares de tarjetas relacionados.</p>
<p>6.3.6 Eliminación de las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación antes que las aplicaciones se activen o se pongan a disposición de los clientes</p>	<p>Las cuentas, los ID de usuario y las contraseñas personalizadas de la aplicación se deben eliminar del código de producción antes de que la aplicación se active o se ponga a disposición de los clientes, ya que estos elementos pueden revelar información sobre el funcionamiento de la aplicación. La posesión de esta información puede poner en riesgo la aplicación y los datos de titulares de tarjetas relacionados.</p>
<p>6.3.7 Revisión del código personalizado antes del envío a producción o a los clientes a fin de identificar posibles vulnerabilidades de la codificación</p> <p><i>Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema que el Requisito 6.3 de las DSS de la PCI exige. Las revisiones de los códigos pueden ser realizadas por personal interno con conocimiento. Las aplicaciones web también están sujetas a controles adicionales, si son públicas, a los efectos de tratar con las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las DSS de la PCI.</i></p>	<p>En general, las personas malintencionadas explotan las vulnerabilidades de los códigos personalizados para obtener acceso a una red y poner en riesgo los datos de titulares de tarjetas. Quienes tienen conocimiento sobre técnicas de codificación segura deben revisar el código para identificar vulnerabilidades.</p>

Requisito	Guía
<p>6.4 Siga los procedimientos de control de todos los cambios en los componentes del sistema. Los procedimientos deben incluir lo siguiente:</p>	<p>Sin controles de cambio de software adecuados, las funciones de seguridad pueden omitirse de manera inadvertida o deliberada, o volverse inoperables, y es posible que se procesen irregularidades o se introduzcan códigos maliciosos. Si las políticas de personal relacionadas con las verificaciones de antecedentes y los controles de acceso a los sistemas no son adecuadas, existe el riesgo de que individuos poco fiables y faltos de formación tengan acceso ilimitado a los códigos de software; los empleados cesantes pueden tener la oportunidad de poner en riesgo los sistemas y es posible que no se detecten acciones no autorizadas.</p>
<p>6.4.1 Documentación de incidencia</p>	<p>El impacto del cambio debe documentarse para que todas las partes afectadas puedan programar de manera apropiada cualquier cambio de procesamiento.</p>
<p>6.4.2 Aprobación de la gerencia a cargo de las partes pertinentes</p>	<p>La aprobación de la gerencia indica que el cambio es legítimo y está autorizado por la organización.</p>
<p>6.4.3 Pruebas de la funcionalidad operativa</p>	<p>Se deben realizar pruebas rigurosas para verificar que todas las acciones son las esperadas, que los informes son precisos, que todas las posibles condiciones de error reaccionan adecuadamente, etc.</p>
<p>6.4.4 Procedimientos de desinstalación</p>	<p>Para cada cambio, debe haber procedimientos de desinstalación en caso de que el cambio falle, para permitir que se pueda volver al estado previo.</p>
<p>6.5 Desarrolle todas las aplicaciones web (internas y externas, que incluyan acceso administrativo web a la aplicación) basadas en las directrices de codificación segura, como la Guía para proyectos de seguridad de aplicaciones web abierta. Considere la prevención de las vulnerabilidades de codificación comunes en los procesos de desarrollo de software, a fin de incluir:</p> <p><i>Nota: Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el punto 6.5.10 se actualizaron en la guía OWASP cuando se publicó la v1.2 de las DSS de la PCI. Sin embargo, al actualizar la guía OSWAP, y si se actualiza, la versión actual se debe utilizar para estos requisitos.</i></p>	<p>La capa de aplicación es de alto riesgo y puede ser el blanco de amenazas internas y externas. Sin la seguridad apropiada, se pueden exponer los datos de titulares de tarjetas y otra información confidencial de la empresa, lo que puede ocasionar daños a la empresa, a sus clientes y a su reputación.</p>

Requisito	Guía
<p>6.5.1 Lenguaje de comandos entre distintos sitios (XSS)</p>	<p>Todos los parámetros deben ser validados antes de su inclusión. Los errores de XSS se producen cuando una aplicación toma datos suministrados por el usuario y los envía a un explorador web sin primero validar o codificar ese contenido. XSS permite a los atacantes ejecutar secuencias en el navegador de la víctima que puede apropiarse de las sesiones del usuario, destruir sitios web y posiblemente introducir gusanos, etc.</p>
<p>6.5.2 Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección LDAP y Xpath, así como otros errores de inyección.</p>	<p>Valide la entrada para verificar que los datos del usuario no pueden modificar el significado de los comandos ni el de las consultas. Los errores de inyección, en especial, los errores de inyección SQL son comunes en las aplicaciones web. La inyección se produce cuando se envían datos suministrados por el usuario a un intérprete como parte de un comando o una consulta. Los datos hostiles del atacante engañan al intérprete para que ejecute comandos accidentales o cambie datos, y le permiten atacar los componentes que hay dentro de la red a través de la aplicación, para iniciar ataques como desbordamientos de buffer o para revelar información confidencial y la funcionalidad de la aplicación del servidor. Ésta también es una forma generalizada de realizar transacciones fraudulentas en sitios web habilitados para el comercio. La información de solicitudes web debe validarse antes de enviarse a la aplicación web; por ejemplo, mediante la verificación de todos los caracteres alfa, la combinación de caracteres numéricos y alfa, etc.</p>
<p>6.5.3 Ejecución de archivos maliciosos</p>	<p>Valide la entrada para verificar que la aplicación no acepte nombres de archivos inesperados ni archivos de los usuarios. El código vulnerable a la inclusión de archivos remotos permite a los atacantes incluir datos y códigos hostiles, lo que genera ataques devastadores, como el riesgo total del servidor. Los ataques por ejecución de archivos maliciosos afectan PHP, XML y cualquier marco que acepte nombres de archivos o archivos de los usuarios.</p>
<p>6.5.4 Referencias inseguras a objetos directos</p>	<p>No exponga referencias a objetos internos ante los usuarios. Una referencia a un objeto directo se produce cuando un desarrollador expone una referencia a un objeto de implementación interna, por ejemplo, un archivo, un directorio, un registro de base de datos o una clave, como un URL o un parámetro de forma. Los atacantes pueden manipular estas referencias para acceder a otros objetos sin autorización.</p>

Requisito	Guía
<p>6.5.5 Falsificación de solicitudes entre distintos sitios (CSRF)</p>	<p>No confíe en las credenciales de autorización ni en los tokens que los exploradores presentan automáticamente. Un ataque de CSRF obliga al navegador de la víctima conectada a enviar una solicitud preautenticada a una aplicación web vulnerable, que luego obliga al navegador de la víctima a ejecutar una acción hostil para beneficio del atacante. La CSRF puede ser tan poderosa como la aplicación web que ataca.</p>
<p>6.5.6 Filtración de información y manejo inadecuado de errores</p>	<p>No filtre información por medio de mensajes de error u otros medios. Las aplicaciones pueden filtrar información sobre su configuración o trabajos internos sin querer o pueden violar la privacidad a través de una variedad de problemas de aplicaciones. Los atacantes usan esta debilidad para robar datos confidenciales o para realizar ataques más graves. Además, el manejo inadecuado de errores ofrece información que ayuda a las personas malintencionadas a poner en riesgo el sistema. Si una persona malintencionada puede crear errores que una aplicación web no puede manejar correctamente, puede obtener información detallada del sistema, puede crear interrupciones por negación de servicios, puede hacer que la seguridad falle o puede bloquear el servidor. Por ejemplo, el mensaje "la contraseña suministrada es incorrecta" indica a los delincuentes que el ID de usuario suministrada es correcto y que deben concentrar sus esfuerzos sólo en la contraseña. Use mensajes de error más genéricos, como "no se pueden verificar los datos".</p>
<p>6.5.7 Autenticación y administración de sesión interrumpidas</p>	<p>Autentique correctamente a los usuarios y proteja las credenciales de cuentas y los tokens de sesión. Por lo general, las credenciales de cuentas y los tokens de sesión no se protegen de manera adecuada. Los atacantes ponen el riesgo las contraseñas, las claves o los tokens de autenticación para asumir la identidad de otros usuarios.</p>
<p>6.5.8 Almacenamiento criptográfico inseguro</p>	<p>Prevenga errores criptográficos. Las aplicaciones web casi nunca usan funciones criptográficas de manera adecuada para proteger los datos y las credenciales. Los atacantes usan estos datos débilmente protegidos para ejecutar robos de identidad y otros delitos, como el fraude de tarjeta de crédito.</p>
<p>6.5.9 Comunicaciones inseguras</p>	<p>Cifre correctamente todas las comunicaciones autenticadas y confidenciales. Con frecuencia, las aplicaciones no cifran el tránsito de la red cuando es necesario proteger comunicaciones confidenciales.</p>

Requisito	Guía
<p>6.5.10 Omisión de restringir el acceso URL</p>	<p>Refuerce constantemente el control del acceso en la capa de presentación y la lógica comercial para todas las URL. Con frecuencia, una aplicación sólo protege la funcionalidad confidencial; para ello, no permite a los usuarios no autorizados que vean vínculos o URL. Los atacantes pueden usar esta debilidad para tener acceso y realizar operaciones no autorizadas mediante el acceso a esos URL directamente.</p>
<p>6.6 En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente y asegúrese de que estas aplicaciones estén protegidas contra ataques conocidos a través de alguno de los siguientes métodos:</p> <ul style="list-style-type: none"> ▪ Controlar las aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, por lo menos, anualmente y después de cada cambio ▪ Instalar un firewall de aplicación web enfrente de aplicaciones web públicas 	<p>En general, los ataques a aplicaciones web son comunes tienen éxito y están permitidos por las malas prácticas de codificación. Este requisito para revisar aplicaciones o instalar firewalls de aplicación web pretende reducir en gran medida la cantidad de riesgos que corren las aplicaciones web públicas que ocasionan fallos en los datos de titulares de tarjetas.</p> <ul style="list-style-type: none"> ▪ Puede usar herramientas o métodos de evaluación de seguridad de vulnerabilidad automáticos o manuales que revisen o examinen las vulnerabilidades de las aplicaciones para cumplir con este requisito. ▪ Los firewalls de aplicación web filtran y bloquean el tránsito no esencial en la capa de aplicación. Junto con un firewall de red, un firewall de aplicación web correctamente configurado previene ataques a la capa de aplicación si las aplicaciones están codificadas o configuradas incorrectamente. <p>Consulte el <i>Suplemento informativo: aclaración del requisito 6.6 sobre revisiones de aplicaciones y firewalls de aplicación web</i> (www.pcisecuritystandards.org), para obtener más información.</p>

Guía para los requisitos 7, 8 y 9: Implemente medidas sólidas de control de acceso

Requisito 7: Restrinja el acceso a datos de titulares de tarjetas sólo a la necesidad de conocimiento de la empresa.

A los efectos de asegurar que el personal autorizado sea el único que pueda acceder a los datos importantes, se deben implementar sistemas y procesos que limiten el acceso conforme a la necesidad de conocer y conforme a la responsabilidad del cargo. "La necesidad de conocer" es la situación en que se otorgan derechos a la menor cantidad de datos y privilegios necesarios para realizar una tarea.

Requisito	Guía
<p>7.1 Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso. Las limitaciones al acceso deben incluir lo siguiente:</p> <p>7.1.1 Restricciones a los derechos de acceso a ID de usuarios privilegiadas a la menor cantidad de privilegios necesarios para cumplir con las responsabilidades del cargo</p> <p>7.1.2 La asignación de privilegios se basa en la tarea del personal individual, su clasificación y función</p> <p>7.1.3 Los requisitos de un formulario de autorización escrito por la gerencia que detalle los privilegios solicitados</p> <p>7.1.4 Implementación de un sistema de control de acceso automático</p>	<p>Mientras más gente tenga acceso a los datos de titulares de tarjetas, más riesgo hay de que una cuenta de usuario se use maliciosamente. Limitar el acceso a quienes tienen una razón comercial sólida para tener acceso ayuda a su organización a prevenir el mal manejo de los datos de titulares de tarjetas por falta de experiencia o maldad. Cuando se otorgan derechos de acceso a la menor cantidad de datos y privilegios necesarios para realizar una tarea, se denomina "necesidad de conocer" y cuando los privilegios se asignan a individuos en base a la clasificación y la función, se denomina "control de acceso basado en funciones" o RBAC. Su organización debe crear una política clara y procesos para el control de acceso a datos en base a la "necesidad de conocer" y mediante el uso del "control de acceso basado en funciones" para definir cómo y a quién se le otorga acceso.</p>
<p>7.2 Establezca un mecanismo para componentes del sistema con múltiples usuarios que restrinja el acceso en base a la necesidad del usuario de conocer y se configure para "negar todos", salvo que se permita particularmente. Este sistema de control de acceso debe incluir lo siguiente:</p> <p><i>Nota: "La necesidad de conocer" es la situación en que se otorgan derechos a la menor cantidad de datos y privilegios necesarios para realizar una tarea.</i></p> <p>7.2.1 Cobertura de todos los componentes del sistema</p> <p>7.2.2 La asignación de privilegios a individuos se basa en la clasificación del trabajo y la función</p> <p>7.2.3 Ajuste predeterminado "negar todos"</p>	<p>Sin un mecanismo para restringir el acceso en base a la necesidad de conocer que tiene el usuario, es posible que sin saberlo se le otorgue acceso a los datos de titulares de tarjetas a un usuario. El uso de un mecanismo o sistema de control de acceso automático es esencial para administrar varios usuarios. Este sistema debe establecerse de acuerdo con la política y los procesos de control de acceso de su organización (incluida la "necesidad de conocer" y el "control de acceso basado en funciones"), debe administrar el acceso a todos los componentes del sistema y debe tener un ajuste predeterminado de "negar todos" para garantizar que a nadie se le otorgue acceso a menos que se establezca una norma específica que le otorgue dicho acceso.</p>

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

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

Requisito	Guía
<p>8.1 Asigne a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema y a datos de titulares de tarjetas.</p>	<p>Si una organización se asegura que cada usuario tiene una identificación única (en vez de usar una misma ID para varios empleados), puede mantener la responsabilidad individual de las acciones y una pista de auditorías efectiva por empleado. Esto ayuda a acelerar la resolución de problemas y la contención cuando se producen malos usos o intenciones malintencionadas.</p>
<p>8.2 Además de la asignación de una ID única, emplee al menos uno de los métodos siguientes para autenticar a los usuarios:</p> <ul style="list-style-type: none"> ▪ Contraseña o frase de seguridad ▪ Autenticación de dos factores (por ejemplo, dispositivos token, tarjetas inteligentes, biometría o claves públicas) 	<p>Estos elementos de autenticación, cuando se usan además de las ID únicas, ayudan a impedir que las ID únicas de los usuarios corran riesgos (ya que quien intenta poner en riesgo las ID necesita saber el ID único y la contraseña u otro elemento de autenticación).</p>
<p>8.3 Incorpore la autenticación de dos factores para el acceso remoto (acceso en el nivel de la red que se origina fuera de la red) a la red de empleados, administradores y terceros. Utilice tecnologías tales como autenticación remota y servicio dial-in (RADIUS); sistema de control de acceso mediante control del acceso desde terminales (TACACS) con tokens; o VPN (basada en SSL/TLS o IPSEC) con certificados individuales.</p>	<p>La autenticación de dos factores requiere dos formas de autenticación para los accesos de mayor riesgo, como los que se originan fuera de su red. Para mayor seguridad, su organización también puede considerar usar autenticación de dos factores cuando accede a redes de mayor seguridad desde redes de menor seguridad; por ejemplo, desde escritorios de la empresa (baja seguridad) a bases de datos/servidores de producción con datos de titulares de tarjetas (alta seguridad).</p>
<p>8.4 Deje ilegibles todas las contraseñas durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una criptografía sólida (se define en el <i>Glosario de términos, abreviaturas y acrónimos de las PCI DS</i>).</p>	<p>Muchas aplicaciones y dispositivos de red transmiten el ID de usuario y la contraseña no cifrada por la red y también almacenan contraseñas sin cifrado. Una persona malintencionada puede fácilmente interceptar la contraseña y el ID de usuario no cifrados o legibles durante la transmisión mediante un "olfateador" o acceder directamente a los ID de usuario y a las contraseñas no cifradas en los archivos donde están almacenadas y usar estos datos robados para obtener acceso no autorizado.</p>

Requisito	Guía
8.5 Asegúrese de que sean correctas la autenticación del usuario y la administración de contraseñas de usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:	Debido a que uno de los primeros pasos que una persona malintencionada dará para poner en riesgo un sistema es explotar las contraseñas débiles o no existentes, es importante implementar buenos procesos para la autenticación del usuario y la administración de las contraseñas.
8.5.1 Controle el agregado, la eliminación y la modificación de las ID de usuario, las credenciales, entre otros objetos de identificación.	Para asegurarse de que los usuarios agregados a sus sistemas son todos usuarios reconocidos y válidos, un pequeño grupo con autoridad específica debe administrar el agregado, la eliminación y la modificación de las ID de usuario. La capacidad de administrar estas ID de usuario sólo debe limitarse a un grupo pequeño.
8.5.2 Verifique la identidad del usuario antes de restablecer contraseñas.	Muchas personas malintencionadas usan la “ingeniería social” (por ejemplo, llaman a una mesa de ayuda y se hacen pasar por usuarios legítimos) para cambiar la contraseña y poder utilizar una ID de usuario. Considere el uso de una “pregunta secreta” que sólo el usuario apropiado pueda responder para ayudar a los administradores a identificar el usuario antes de borrar las contraseñas. Asegúrese de que las preguntas estén correctamente aseguradas y no se compartan.
8.5.3 Configure la primera contraseña en un valor único para cada usuario y cámbiela de inmediato después del primer uso.	Si se usa la misma contraseña para todas las nuevas configuraciones de usuario, un usuario interno, un ex empleado o una persona malintencionada pueden saber o descubrir fácilmente esta contraseña y usarla para obtener acceso a cuentas.
8.5.4 Cancele de inmediato el acceso para cualquier usuario cesante.	Si un empleado se va de la empresa y aún tiene acceso a la red con su cuenta de usuario, se puede producir un acceso innecesario o malintencionado a los datos de titulares de tarjetas. El autor de este acceso puede ser un ex empleado o un usuario malintencionado que explota una cuenta antigua o que no se usa. Considere implementar un proceso con Recursos Humanos para que se realice una notificación inmediata cuando un empleado queda cesante para que la cuenta de usuario se desactive rápidamente.
8.5.5 Elimine/desactive las cuentas de usuario cada 90 días, como mínimo.	La existencia de cuentas inactivas permite a un usuario no autorizado explotar la cuenta que no se usa para poder acceder a los datos de titulares de tarjetas.

Requisito	Guía
<p>8.5.6 Active las cuentas que utilicen los proveedores para el mantenimiento remoto únicamente durante el período necesario.</p>	<p>Si permite que los proveedores (como los proveedores de POS) tengan acceso a su red las 24 horas, todos los días, cuando necesitan realizar el soporte de sus sistemas, aumentarán las posibilidades de acceso no autorizado, ya sea de un usuario del entorno de proveedores o de un individuo malintencionado que encuentra y usa este punto siempre listo de acceso externo a la red. Consulte también 12.3.8 y 12.3.9 para obtener más información sobre este tema.</p>
<p>8.5.7 Informe los procedimientos y las políticas de contraseñas a todos los usuarios que tengan acceso a datos de titulares de tarjetas.</p>	<p>Comunicar los procedimientos de contraseñas a todos los usuarios ayuda a esos usuarios a comprender y acatar las políticas y a estar alertas a cualquier individuo malintencionado que puede intentar explotar sus contraseñas para obtener acceso a los datos de titulares de tarjetas (por ejemplo, llamando a un empleado y solicitándole su contraseña para que quien llama pueda “resolver un problema”).</p>
<p>8.5.8 No utilice cuentas ni contraseñas grupales, compartidas o genéricas.</p>	<p>Si varios usuarios comparten la misma cuenta y la misma contraseña, se torna imposible asignar responsabilidad o tener un registro efectivo de las acciones de un individuo, ya que una acción específica puede haber sido realizada por cualquier persona del grupo que comparte la cuenta y la contraseña.</p>
<p>8.5.9 Cambie las contraseñas de usuario al menos cada 90 días.</p>	<p>Las contraseñas fuertes son la primera línea de defensa de una red ya que, generalmente, un individuo malintencionado primero intentará obtener acceso a cuentas con contraseñas débiles o no existentes. Un individuo malintencionado tiene más tiempo para encontrar estas cuentas débiles y poner en riesgo una red con la apariencia de una ID de usuario válida, si las contraseñas son breves, fáciles de adivinar o válidas durante un largo tiempo sin cambiar. Las contraseñas fuertes pueden hacerse valer y mantenerse según estos requisitos porque admiten las funciones de seguridad de contraseñas y cuentas incluidas con el sistema operativo (por ejemplo, Windows), las redes, las bases de datos y otras plataformas.</p>
<p>8.5.10 Solicite una longitud de contraseña mínima de siete caracteres.</p>	
<p>8.5.11 Utilice contraseñas que contengan tanto caracteres numéricos como alfabéticos.</p>	
<p>8.5.12 No permita que ninguna persona envíe una contraseña nueva igual a cualquiera de las últimas cuatro contraseñas utilizadas.</p>	
<p>8.5.13 Limite los intentos de acceso repetidos mediante el bloqueo del ID de usuario después de más de seis intentos.</p>	<p>Sin la implementación de mecanismos de cierre de cuenta, un atacante puede intentar constantemente adivinar una contraseña a través de herramientas manuales o automáticas (por ejemplo, el craqueo de contraseñas), hasta que logre descifrarla y obtenga acceso a una cuenta de usuario.</p>

Requisito	Guía
<p>8.5.14 Establezca la duración del bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite el ID de usuario.</p>	<p>Si una cuenta está bloqueada debido a que alguien intenta constantemente adivinar una contraseña, los controles para demorar la reactivación de estas cuentas bloqueadas detienen al individuo malintencionado para que no pueda seguir adivinando constantemente la contraseña (tendrá que esperar al menos 30 minutos hasta que la cuenta se reactive). Además, si es necesario solicitar la reactivación, la mesa de ayuda o admin pueden validar que el propietario de la cuenta es la causa (por errores de tipeo) del bloqueo.</p>
<p>8.5.15 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para que se active la terminal nuevamente.</p>	<p>Cuando los usuarios se alejan de una máquina encendida con acceso a datos importantes de red o de titulares de tarjetas, esa máquina puede ser usada por otras personas durante la ausencia del usuario, lo que puede ocasionar un acceso no autorizado a cuentas o un mal uso de cuentas.</p>
<p>8.5.16 Autentique todos los accesos a cualquier base de datos que contenga datos de titulares de tarjetas. Esto incluye el acceso de aplicaciones, administradores y demás usuarios.</p>	<p>Sin la autenticación del usuario para acceder a bases de datos y aplicaciones, la posibilidad de acceso no autorizado o malintencionado aumenta, y dicho acceso no puede ser registrado porque el usuario no ha sido autenticado y, por lo tanto, el sistema no lo reconoce. Además, el acceso a la base de datos debe otorgarse sólo a través de métodos programáticos (por ejemplo, a través de procedimientos almacenados), en vez de a través de acceso directo a las bases de datos por parte de los usuarios finales (excepto para los DBA, que pueden tener acceso directo a la base de datos para sus funciones administrativas).</p>

Requisito 9: Limite el acceso físico a los datos del titular de la tarjeta

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

Requisito	Guía
<p>9.1 Utilice controles de entrada a la empresa para limitar y supervisar el acceso a sistemas en el entorno de datos de titulares de tarjetas.</p>	<p>Sin controles de acceso físico, las personas no autorizadas pueden obtener acceso al edificio y a información confidencial, y pueden alterar las configuraciones del sistema, introducir vulnerabilidades en la red o destruir o robar computadoras.</p>
<p>9.1.1 Utilice cámaras de video u otros mecanismos de control de acceso para supervisar el acceso físico de personas a áreas confidenciales. Revise los datos recopilados y correlaciónelos con otras entradas. Guárdelos durante al menos tres meses, a menos que la ley estipule lo contrario.</p> <p><i>Nota: “Áreas confidenciales” hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan datos de titulares de tarjetas. No se incluyen las áreas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.</i></p>	<p>Cuando se investigan fallos físicos, estos controles pueden ayudar a identificar individuos que tienen acceso físico a esas áreas que almacenan datos de titulares de tarjetas.</p>
<p>9.1.2 Restrinja el acceso físico a conexiones de red de acceso público.</p>	<p>Si se restringe el acceso a conexiones de red, se impide que personas malintencionadas tengan acceso a las conexiones de red disponibles que pueden permitirles acceder a recursos de red internos. Considere cerrar las conexiones de red cuando no las use y reactivarlas sólo cuando sean necesarias. En las áreas públicas, como las salas de conferencias, establezca redes privadas para permitir a los proveedores y visitantes tener acceso sólo a Internet para que accedan a su red interna.</p>
<p>9.1.3 Restrinja el acceso físico a puntos de acceso inalámbrico, puertas de enlace y dispositivos manuales.</p>	<p>Sin seguridad en el acceso a los dispositivos y componentes inalámbricos, los usuarios malintencionados pueden usar los dispositivos inalámbricos sin vigilancia de su empresa para acceder a los recursos de red o, incluso, conectar sus propios dispositivos a la red inalámbrica, lo que les da acceso no autorizado. Considere establecer puntos de acceso inalámbrico y puertas de enlace en áreas de almacenamiento seguro, como dentro de armarios cerrados o salas de servidores. Asegúrese de que el cifrado sólido esté habilitado. Habilite el bloqueo automático de dispositivos en dispositivos manuales inalámbricos después de un período inactivo prolongado y configure los dispositivos para que soliciten una contraseña cuando se los enciende.</p>

Requisito	Guía
<p>9.2 Desarrolle procedimientos para que el personal pueda distinguir con facilidad entre empleados y visitantes, especialmente en las áreas donde se puede acceder fácilmente a datos de titulares de tarjetas.</p> <p><i>A los fines de este requisito, "empleados" se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que "residan" en las instalaciones de la entidad. "Visitante" se define como proveedor, invitado de algún empleado, personal de servicio o cualquier persona que necesite ingresar a las instalaciones de la empresa durante un tiempo no prolongado, generalmente no más de un día.</i></p>	<p>Sin sistemas de placas de identificación y controles de puertas, los usuarios no autorizados y malintencionados fácilmente pueden obtener acceso a su instalación y robar, desactivar, afectar o destruir sistemas importantes y datos de titulares de tarjetas. Para un control óptimo, considere implementar un sistema de acceso con tarjetas o placas de identificación para ingresar y salir a las áreas de trabajo que contienen datos de titulares de tarjetas.</p>
<p>9.3 Asegúrese de que todos los visitantes reciban el siguiente trato:</p>	<p>Los controles que se realizan a visitantes son importantes para reducir las posibilidades de que personas no autorizadas o malintencionadas obtengan acceso a sus instalaciones (y posiblemente, tengan acceso a datos de los titulares de tarjetas).</p>
<p>9.3.1 Autorización previa al ingreso a áreas en las que se procesan o se conservan datos de titulares de tarjetas</p> <p>9.3.2 Token físico otorgado (por ejemplo una placa de identificación o dispositivo de acceso) con vencimiento y que identifique a los visitantes como personas no pertenecientes a la empresa.</p> <p>9.3.3 Solicitud de entrega del token físico antes de salir de las instalaciones de la empresa o al momento del vencimiento.</p>	<p>Los controles que se realizan a visitantes son importantes para garantizar que éstos sólo ingresen a áreas a las que están autorizados a ingresar, que se los identifique como visitantes para que los empleados puedan controlar sus actividades y que su acceso esté restringido sólo a la duración de su visita legítima.</p>
<p>9.4 Use un registro de visitas para implementar una pista de auditoría física de la actividad de visitas. Documente el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico en el registro. Conserve este registro durante tres meses como mínimo, a menos que la ley estipule lo contrario.</p>	<p>Es simple y económico mantener un registro de visitantes que documente información mínima sobre el visitante y, en una posible investigación de fallo de datos, ayuda a identificar el acceso físico a un edificio o a una sala y el posible acceso a datos de titulares de tarjetas. Considere implementar registros en el ingreso a instalaciones y, en particular, en el ingreso a zonas donde hay datos de titulares de tarjetas.</p>
<p>9.5 Almacene los medios de copias de seguridad en un lugar seguro, preferentemente en un lugar externo a la empresa, como un centro alternativo o para copias de seguridad, o un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo.</p>	<p>Si las copias de seguridad que contienen datos de titulares de tarjetas están almacenadas en una instalación no asegurada, se pueden perder con facilidad o pueden ser robadas o copiadas con malas intenciones. Para un almacenamiento seguro, considere contratar una empresa de almacenamiento de datos comerciales o, en si la empresa es más pequeña, use una caja de seguridad en un banco.</p>

Requisito	Guía
9.6 Resguarde de forma física todos los papeles y dispositivos electrónicos que contengan datos de titulares de tarjetas.	Los datos de titulares de tarjetas son propensos a que personas no autorizadas los vean, copien o escaneen, si no están protegidos cuando están en medios portátiles, impresos o se dejan en algún escritorio. Considere la implementación de procedimientos y procesos para proteger los datos de titulares de tarjetas en medios distribuidos a usuarios internos o externos. Sin estos procedimientos, los datos se pueden perder o pueden ser robados y usados para fines fraudulentos.
9.7 Lleve un control estricto sobre la distribución interna o externa de cualquier tipo de medios que contenga datos de titulares de tarjetas, incluidos:	
9.7.1 Clasifique los medios de manera que se puedan identificar como confidenciales.	Es posible que los medios que no se identifican como confidenciales no reciban el cuidado que requieren, de manera pueden ser robados o se pueden perder. Incluya un proceso de clasificación de medios en los procedimientos que se recomiendan en el Requisito 9.6.
9.7.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.	Si los medios son enviados a través de un método que no se puede rastrear, como el correo postal común, pueden ser robados o los pueden robar. Use los servicios de un correo seguro para entregar todos los medios que contienen datos de titulares de tarjetas, a fin de poder usar los sistemas de rastreo para tener un inventario y poder ubicar los envíos.
9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura (especialmente cuando se los distribuye a personas).	Los datos de titulares de tarjetas que salen de áreas seguras sin un proceso aprobado por la gerencia pueden perderse o es posible que los roben. Sin un proceso firme, no se rastrean las ubicaciones de los medios ni existe un procedimiento para saber dónde van los datos o cómo se protegen. Incluya la creación de un proceso aprobado por la gerencia para mover los medios en los procedimientos que se recomiendan en el Requisito 9.6.
9.9 Lleve un control estricto sobre el almacenamiento y la accesibilidad de los medios que contengan datos de titulares de tarjetas.	Sin métodos de inventarios y controles de almacenamiento cuidadosos, los medios robados o perdidos pueden pasar inadvertidos durante un período de tiempo indefinido. Incluya el desarrollo de un proceso para limitar el acceso a los medios con datos de titulares de tarjetas en los procedimientos que se recomiendan en el Requisito 9.6.
9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	Si no se realiza un inventario de los medios, los que se pierden o son robados pueden pasar inadvertidos durante un largo tiempo. Incluya la creación de un proceso para inventarios de medios y almacenamiento seguro en los procedimientos que se recomiendan en el Requisito 9.6.

Requisito	Guía
9.10 Destruya los medios que contengan datos de titulares de tarjetas cuando ya no sea necesario para la empresa o por motivos legales, de la siguiente manera:	Si no se toman medidas para destruir la información que se almacena en los discos duros de las computadoras, en los CD y en papel, la disposición de esa información puede ocasionar riesgos y provocar pérdidas económicas o de reputación. Por ejemplo, personas malintencionadas pueden usar una técnica conocida como “buscar en la basura”, en donde buscan en contenedores de basura y papeleras de reciclaje y usan la información que encuentran para lanzar un ataque. Incluya el desarrollo de una proceso para destruir los medios con datos de titulares de tarjetas, incluido el almacenamiento adecuado de estos medios antes de su destrucción, en los procedimientos que se recomiendan en el Requisito 9.6.
9.10.1 Corte en tiras, incinere o haga pasta los materiales de copias en papel para que no se puedan reconstruir los datos de titulares de tarjetas.	
9.10.2 Entregue los datos de titulares de tarjetas en dispositivos electrónicos no recuperables para que dichos datos no se puedan reconstruir.	

Guía para los requisitos 10 y 11: Supervise y pruebe las redes con regularidad

Requisito 10: Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas

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

Requisito	Guía
<p>10.1 Establezca un proceso para vincular todos los accesos a componentes del sistema (especialmente el acceso con privilegios administrativos, tales como de raíz) a cada usuario en particular.</p>	<p>Es fundamental tener un proceso o un sistema que vincule el acceso de los usuarios con los componentes del sistema a los que se ha accedido y, en particular, para esos usuarios con privilegios administrativos. Este sistema genera registros de auditoría y ofrece la posibilidad de realizar un seguimiento de las actividades sospechosas de un usuario específico. Los equipos forenses posincidentes dependen mucho de estos registros para comenzar su investigación.</p>
<p>10.2 Implemente pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos:</p> <ul style="list-style-type: none"> 10.2.1 Todo acceso de personas a datos de titulares de tarjetas 10.2.2 Todas las acciones realizadas por personas con privilegios de raíz o administrativos 10.2.3 Acceso a todas las pistas de auditoría 10.2.4 Intentos de acceso lógico no válidos 10.2.5 Uso de mecanismos de identificación y autenticación 10.2.6 Inicialización de los registros de auditoría 10.2.7 Creación y eliminación de objetos en el nivel del sistema. 	<p>En general, las personas malintencionadas que entran en la red efectúan muchos intentos para acceder a los sistemas objetivos. La generación de pistas de auditoría de las actividades sospechosas alerta al administrador del sistema, envía datos a otros mecanismos de monitorización (como los sistemas de detección de intrusiones) y ofrece un historial de pistas para un seguimiento posincidente.</p>

Requisito	Guía
<p>10.3 Registre al menos las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:</p> <ul style="list-style-type: none"> 10.3.1 Identificación de usuarios 10.3.2 Tipo de evento 10.3.3 Fecha y hora 10.3.4 Indicación de éxito u omisión 10.3.5 Origen del evento 10.3.6 Identidad o nombre de los datos, componentes del sistema o recurso afectados 	<p>Si registra estas entradas para los eventos auditables de 10.2, cualquier posibilidad de riesgo puede identificarse rápidamente y con suficientes detalles como para saber quién fue, qué hizo, dónde lo hizo y cómo lo hizo.</p>
<p>10.4 Sincronice todos los relojes y horarios críticos del sistema.</p>	<p>En general, si un individuo malintencionado ingresa en la red, intenta cambiar los sellos de fecha de sus acciones dentro de los registros de auditoría para impedir que detecten su actividad. Para los equipos forenses posincidentes, la hora de cada actividad es esencial para determinar cómo se puso en riesgo los sistemas. Una persona malintencionada también puede intentar cambiar directamente el reloj de un servidor de hora, si las restricciones de acceso no son las apropiadas, para volver a colocar la hora que había antes de que el individuo malintencionado ingresara a la red.</p>
<p>10.5 Resguede las pistas de auditoría para evitar que se modifiquen.</p>	<p>Por lo general, un individuo malintencionado que ingresa a una red intenta editar los registros de auditoría para ocultar su actividad. Sin la protección adecuada de los registros de auditoría, no se puede garantizar su integridad ni exactitud, y los registros de auditoría pueden resultar inútiles como herramienta de investigación después de que han estado en riesgo.</p>
<ul style="list-style-type: none"> 10.5.1 Limite la visualización de pistas de auditoría a quienes lo necesiten por motivos de trabajo. 10.5.2 Proteja los archivos de las pistas de auditoría contra las modificaciones no autorizadas. 10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de inmediato en un servidor de registros central o medios que resulten difíciles de modificar. 10.5.4 Escriba registros para tecnologías externas en un servidor de registros en la LAN interna. 	<p>La protección adecuada de los registros de auditoría incluye un fuerte control de acceso (acceso limitado a registros sólo en base a la “necesidad de conocer”) y el uso de segregación interna (para hacer que los registros sean más difíciles de encontrar y modificar). Si los registros se escriben desde tecnologías externas como inalámbricas, firewalls, DNS y servidores de correo, se reduce el riesgo de que esos registros se pierdan o se alteren, ya que son más seguros dentro de la red interna.</p>

Requisito	Guía
<p>10.5.5 Utilice el software de monitorización de integridad de archivos y de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).</p>	<p>Los sistemas de monitorización de integridad de archivos verifican los cambios que se realizan en los archivos importantes y notifican cuando se observan esos cambios. A los fines de la monitorización de integridad de archivos, una entidad generalmente monitorea los archivos que no se modifican regularmente, pero que cuando se modifican indican un posible riesgo. En el caso de los archivos de registro (que no cambian con frecuencia), lo que debe monitorearse es, por ejemplo, cuando se elimina un archivo, las disminuciones o los aumentos repentinos y cualquier otro indicador de que un individuo malintencionado ha alterado un archivo de registro. Existen herramientas de forma estándar y de código abierto disponibles para la monitorización de integridad de archivos.</p>
<p>10.6 Revise los registros de todos los componentes del sistema al menos una vez al día. Las revisiones de registros incluyen a los servidores que realizan funciones de seguridad, tales como sistema de detección de intrusiones (IDS) y servidores de autenticación, autorización y contabilidad (AAA) (por ejemplo, RADIUS).</p> <p><i>Nota: las herramientas de recolección, análisis y alerta de registros pueden ser utilizadas para cumplir con el requisito 10.6.</i></p>	<p>Existen fallos que son detectados días o meses después. Verificar los registros a diario reduce la cantidad de tiempo y exposición de un posible riesgo. Los procesos de revisión de registro no necesariamente deben ser manuales. Especialmente en el caso de las entidades con una gran cantidad de servidores, considere el uso de herramientas de recolección, análisis y alerta de registros.</p>
<p>10.7 Conserve el historial de pista de auditorías durante al menos un año, con un mínimo de tres meses inmediatamente disponible para el análisis (por ejemplo, en línea, archivado o recuperable para la realización de copias de seguridad).</p>	<p>La conservación de registros durante al menos un año es importante, ya que, en general, transcurre cierto tiempo antes de que se detecte un riesgo, y esto permite a los investigadores contar con un historial de registros lo suficientemente grande para determinar mejor el tiempo de un posible fallo y los posibles sistemas afectados. Si una entidad tiene tres meses de registros inmediatamente disponibles, puede identificar rápidamente el fallo de datos y minimizar su impacto. El almacenamiento de cintas de respaldo en un lugar externo a la empresa puede hacer que se necesite más tiempo para restablecer los datos, realizar análisis e identificar los sistemas o datos que han sido afectados.</p>

Requisito 11: Pruebe los sistemas y procesos de seguridad regularmente

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

Requisito	Guía
<p>11.1 Las pruebas para comprobar la presencia de puntos de acceso inalámbricos mediante el uso de un analizador inalámbrico al menos trimestralmente o la implementación de un sistema de detección de intrusiones (IDS)/sistema contra intrusos (IPS) inalámbrico para identificar todos los dispositivos inalámbricos en uso.</p>	<p>La implementación y explotación de tecnología inalámbrica dentro de una red es una de las vías más comunes para que los usuarios malintencionados obtengan acceso a la red y a los datos de titulares de tarjetas. Si se instala una red o un dispositivo inalámbrico sin que la empresa sepa, un atacante puede ingresar a la red fácilmente y “de manera invisible”. Además de analizadores inalámbricos, se pueden usar análisis de puertos y otras herramientas de red que detectan dispositivos inalámbricos.</p> <p>Debido a la facilidad con la que un punto de acceso inalámbrico puede conectarse a una red, la dificultad para detectar su presencia y el gran riesgo que presentan los dispositivos inalámbricos no autorizados, estos análisis deben realizarse incluso cuando existe una política que prohíbe el uso de tecnología inalámbrica.</p> <p>Una organización debe tener, como parte de su plan de respuesta a incidentes, procedimientos documentados para seguir en caso de que se detecte un punto de acceso inalámbrico no autorizado. Se debe configurar un IDS/IPS inalámbrico para que automáticamente genere una alerta, pero el plan también debe documentar procedimientos de respuesta si se detecta un dispositivo no autorizado durante un análisis inalámbrico manual.</p>
<p>11.2 Realice análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas de firewall, actualizaciones de productos).</p> <p><i>Nota: los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor Aprobado de Escaneo (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC). Los análisis realizados después de cambios en la red puede realizarlos el personal interno de la empresa.</i></p>	<p>Un análisis de vulnerabilidades es una herramienta automática que se utiliza en servidores y dispositivos de red internos y externos, y está diseñada para exponer posibles vulnerabilidades e identificar puertos en redes que personas malintencionadas pueden hallar y explotar. Una vez que estas debilidades son identificadas, la entidad las corrige y repite el análisis para verificar que las vulnerabilidades se hayan corregido.</p> <p>En el momento de una evaluación inicial de PCI DSS en una entidad, es posible que aún no se hayan realizado cuatro análisis trimestrales. Si el resultado del análisis más reciente cumple con los criterios de un análisis aprobado y se han implementado políticas y procedimientos para futuros análisis trimestrales, el objetivo de este requisito se ha logrado. No es necesario demorar una evaluación “implementada” para este requisito por la falta de cuatro análisis si se cumplen estas condiciones.</p>

Requisito	Guía
<p>11.3 Realice pruebas de penetración externas e internas al menos una vez al año y después de cualquier actualización o modificación significativa de infraestructuras o aplicaciones (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor Web al entorno). Estas pruebas de penetración deben incluir lo siguiente:</p> <p>11.3.1 Pruebas de penetración de la capa de red</p> <p>11.3.2 Pruebas de penetración de la capa de aplicación.</p>	<p>Las pruebas de penetración de la red y aplicación son diferentes de los análisis de vulnerabilidades porque las pruebas de penetración son más manuales, intentan explotar algunas de las vulnerabilidades que se identifican en los análisis e incluyen técnicas que usan las personas malintencionadas para aprovechar los procesos o sistemas de seguridad débiles.</p> <p>Antes de que las aplicaciones, los dispositivos de red y los sistemas se comiencen a producir, deben fortalecerse y asegurarse con las mejores prácticas de seguridad (según el Requisito 2.2). Los análisis de vulnerabilidades y las pruebas de penetración exponen todas las vulnerabilidades que quedan y que un atacante puede encontrar y explotar.</p>
<p>11.4 Utilice los sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el entorno de datos de titulares de tarjetas y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores de detección y prevención de intrusiones.</p>	<p>Estas herramientas comparan el tránsito que ingresa a la red con “firmas” conocidas de miles de tipos de riesgos (herramientas de hackers, troyanos y otro malware) y envían alertas o detienen el intento mientras se produce. Sin un enfoque proactivo para la detección de actividades no autorizadas a través de estas herramientas, los ataques a recursos informáticos (o su mal uso) pueden pasar inadvertidos en tiempo real. Las alertas de seguridad que generan estas herramientas pueden monitorearse para que los intentos de intrusiones puedan detenerse.</p> <p>Existen miles de tipos de riesgos y, a diario, se descubren muchos más. Las versiones obsoletas de estos sistemas no tendrán “firmas” actualizadas y no identificarán nuevas vulnerabilidades que pueden provocar un fallo no detectado. Los proveedores de estos productos suministran actualizaciones con frecuencia o, incluso, diariamente.</p>
<p>11.5 Implemente el software de monitorización de integridad de archivos para alertar al personal ante modificaciones no autorizadas de archivos críticos del sistema, archivos de configuración o archivos de contenido; asimismo configure el software para realizar comparaciones de archivos críticos al menos semanalmente.</p> <p><i>Nota: a los fines de la monitorización de integridad de archivos, los archivos críticos generalmente son los que no se modifican con regularidad, pero cuya modificación podría indicar un riesgo o peligro para el sistema. Los productos para la monitorización de integridad de archivos generalmente vienen preconfigurados con archivos críticos para el sistema operativo relacionado. La entidad (es decir el comerciante o el proveedor de servicios) debe evaluar y definir otros archivos críticos, tales como los archivos para aplicaciones personalizadas.</i></p>	<p>Los sistemas de monitorización de integridad de archivos verifican los cambios que se realizan a los archivos importantes y notifican cuando se detectan esos cambios. Existen herramientas de forma estándar y de código abierto disponibles para la monitorización de integridad de archivos. Si la monitorización de integridad de archivos no se implementa correctamente y no se controla su resultado, un individuo malintencionado puede alterar el contenido de los archivos de configuración, los programas de los sistemas operativos o los ejecutables de aplicaciones. Si no se detectan estos cambios no autorizados, los controles de seguridad existentes pueden ser ineficaces o es posible que se roben los datos de titulares de tarjetas sin un impacto perceptible en el procesamiento normal.</p>

Guía para el requisito 12: Mantenga una política de seguridad de información

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

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

Requisito	Guía
<p>12.1 Establezca, publique, mantenga y distribuya una política de seguridad que logre lo siguiente:</p> <ul style="list-style-type: none"> 12.1.1 Aborde todos los requisitos de PCI DSS. 12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos. 12.1.3 Incluya una revisión al menos una vez al año y actualizaciones al modificarse el entorno. 	<p>La política de seguridad de la información de una empresa crea un plan de acción para implementar medidas de seguridad para proteger su activo más valioso. Una política de seguridad sólida establece el grado de seguridad para toda la empresa e informa a los empleados lo que se espera de ellos. Todos los empleados deben estar al tanto de la confidencialidad de los datos y de su responsabilidad para protegerlos.</p> <p>Las amenazas de seguridad y los métodos de protección evolucionan rápidamente durante el año. Si la política de seguridad no se actualiza para reflejar estos cambios, no se implementarán nuevas medidas de protección para luchar contra estas amenazas.</p>
<p>12.2 Desarrolle procedimientos diarios de seguridad operativa coherentes con los requisitos de esta especificación (por ejemplo, procedimientos de mantenimiento de cuentas de usuarios y procedimientos de revisión de registros).</p>	<p>Los procedimientos de seguridad operativa funcionan como “instrucciones de escritorio” para que los trabajadores usen en sus actividades cotidianas de mantenimiento y administración de sistemas. Los procedimientos de seguridad operativa no documentados conducen a trabajadores que no conocen al alcance total de sus tareas, procesos que los trabajadores no pueden repetir fácilmente y posibles brechas en estos procesos que pueden permitir a una persona malintencionada obtener acceso a recursos y sistemas importantes.</p>

Requisito	Guía
<p>12.3 Desarrolle políticas de utilización para tecnologías críticas para empleados (por ejemplo, tecnologías de acceso remoto, tecnologías inalámbricas, dispositivos electrónicos extraíbles, computadoras portátiles, asistentes digitales/para datos personales [PDA], utilización del correo electrónico Internet) para definir el uso adecuado de dichas tecnologías por parte de empleados y contratistas. Asegúrese de que estas políticas de uso requieran lo siguiente:</p>	<p>Las políticas de utilización de los empleados pueden prohibir ciertos dispositivos y otras tecnologías, si es parte de la política de la empresa, u ofrecer orientación para los empleados respecto al correcto uso y la implementación. Si no se implementan políticas de uso, los empleados pueden usar la tecnología para violar la política de la empresa y, así, permitir a personas malintencionadas obtener acceso a sistemas importantes y datos de titulares de tarjetas. Un ejemplo puede ser configurar, sin saberlo, redes inalámbricas sin seguridad. Para garantizar que se sigan las normas de la empresa y que sólo se implemente la tecnología aprobada, considere limitar la implementación sólo a equipos de operaciones y no permitir que empleados generales/no especializados instalen esta tecnología.</p>
<p>12.3.1 Aprobación explícita de la gerencia</p>	<p>Si no se requiere la correcta aprobación de la gerencia para la implementación de estas tecnologías, un empleado puede, de manera inocente, implementar una solución para una necesidad percibida de la empresa, pero también puede abrir un gran agujero que somete a datos y sistemas importantes a personas malintencionadas.</p>
<p>12.3.2 Autenticación para el uso de la tecnología</p>	<p>Si la tecnología se implementa sin una autenticación correcta (ID de usuario y contraseña, tokens, VPN, etc.), los individuos malintencionados pueden usar fácilmente esta tecnología no protegida para acceder a datos de titulares de tarjetas y sistemas importantes.</p>
<p>12.3.3 Lista de todos los dispositivos y personal que tenga acceso</p>	<p>Las personas malintencionadas pueden poner en peligro la seguridad física y colocar sus propios dispositivos en la red como “puerta trasera”. Los empleados también pueden omitir procedimientos e instalar dispositivos. Un inventario preciso con un etiquetado adecuado de los dispositivos permite una rápida identificación de las instalaciones no aprobadas. Considere establecer una convención de nombres oficial para los dispositivos y etiquete y registre todos los dispositivos conjuntamente con los controles de inventario establecidos.</p>
<p>12.3.4 Etiquetado de dispositivos con propietario, información de contacto y objetivo</p>	
<p>12.3.5 Usos aceptables de la tecnología</p>	
<p>12.3.6 Ubicaciones aceptables de las tecnologías en la red</p>	<p>Si se define el uso y la ubicación de la tecnología y los dispositivos aprobados por la empresa, la empresa está mejor capacitada para administrar y controlar las diferencias de configuración y los controles operativos, para asegurarse de que no haya ninguna “puerta trasera” abierta para que personas malintencionadas obtengan acceso a sistemas críticos y datos de titulares de tarjetas.</p>
<p>12.3.7 Lista de productos aprobados por la empresa</p>	

Requisito	Guía
<p>12.3.8 Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad</p>	<p>La tecnología de acceso remoto es una “puerta trasera” frecuente para los datos de titulares de tarjetas y los recursos importantes. Si se desconecta la tecnología de acceso remoto cuando no se utiliza (por ejemplo, la que se usa para que los POS u otros proveedores realicen el soporte de sus sistemas) se reduce el acceso y el riesgo que corren las redes. Considere el uso de controles para desconectar los dispositivos después de 15 minutos de inactividad. Consulte también el Requisito 8.5.6 para obtener más información sobre este tema.</p>
<p>12.3.9 Activación de tecnologías de acceso remoto para proveedores sólo cuando estos lo requieren, con desactivación automática después de la utilización</p>	
<p>12.3.10 Al tener acceso remoto a datos de titulares de tarjetas mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos de titulares de tarjetas en unidades de disco locales y dispositivos electrónicos extraíbles.</p>	
<p>12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todos los empleados y contratistas.</p>	<p>Sin responsabilidades y roles de seguridad claramente definidos y asignados, puede haber una interacción contradictoria con el grupo de seguridad, lo que puede ocasionar una implementación no segura de tecnología o el uso de tecnología no segura u obsoleta.</p>
<p>12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o a un equipo:</p> <p>12.5.1 Establezca, documente y distribuya políticas y procedimientos de seguridad.</p> <p>12.5.2 Supervise y analice las alertas e información de seguridad, y distribúyalas entre el personal correspondiente.</p> <p>12.5.3 Establezca, documente y distribuya los procedimientos de respuesta ante incidentes de seguridad y escalamiento para garantizar un manejo oportuno y efectivo de todas las situaciones.</p> <p>12.5.4 Administre las cuentas de usuario, incluidas las adiciones, eliminaciones y modificaciones.</p> <p>12.5.5 Supervise y controle todo acceso a datos.</p>	<p>Cada persona o equipo con responsabilidades en la gestión de seguridad de la información debe saber muy bien sus responsabilidades y tareas relacionadas, a través de una política específica. Sin esta responsabilidad, las diferencias en los procesos pueden permitir el acceso a datos de titulares de tarjetas y recursos importantes.</p>

Requisito	Guía
<p>12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.</p>	<p>Si no se enseña a los usuarios a ser responsables de la seguridad, los procesos y garantías de seguridad que se han implementado pueden ser ineficientes debido a acciones intencionales o errores de los empleados.</p>
<p>12.6.1 Eduque a los empleados al contratarlos y al menos una vez al año.</p>	<p>Si el programa formal de concienciación no incluye sesiones de actualización anuales, los procedimientos y procesos de seguridad de claves pueden olvidarse u omitirse, lo que hace que los datos de titulares de tarjetas y los recursos importantes queden expuestos.</p>
<p>12.6.2 Exija a los empleados que reconozcan al menos una vez al año haber leído y entendido la política y los procedimientos de seguridad de la empresa.</p>	<p>La solicitud a los empleados de un reconocimiento (por ejemplo: por escrito o de forma electrónica) ayuda a garantizar que hayan leído y comprendido los procedimientos y las políticas de seguridad y que se han comprometido a cumplir con estas políticas.</p>
<p>12.7 Examine a los posibles empleados (consulte la definición de “empleados” en 9.2 más arriba) antes de contratarlos a los fines de minimizar el riesgo de ataques provenientes de orígenes internos. <i>En el caso de empleados tales como cajeros de un comercio, que sólo tienen acceso a un número de tarjeta a la vez al realizarse una transacción, este requisito constituye sólo una recomendación.</i></p>	<p>La realización de investigaciones minuciosas antes de contratar empleados a quienes se les dará acceso a datos de titulares de tarjetas reduce el riesgo del uso no autorizado de PAN y de otros datos de titulares de tarjetas por parte de personas con antecedentes criminales o cuestionables. Se supone que una empresa debe tener una política y un proceso para el control de antecedentes, incluido su propio proceso de decisiones para el que los resultados del control de antecedentes tienen incidencia en las decisiones al momento de contratar personal (y cuál es ese impacto).</p>
<p>12.8 Si los datos de titulares de tarjeta se comparten con proveedores de servicios, mantenga e implemente políticas y procedimientos a los fines de que los proveedores de servicio incluyan lo siguiente:</p>	<p>Si un comerciante o proveedor de servicios comparte datos de titulares de tarjetas con un proveedor de servicios, entonces se aplican ciertos requisitos para garantizar que estos proveedores de servicios respeten una protección constante de estos datos.</p>
<p>12.8.1 Mantenga una lista de proveedores de servicios.</p>	<p>Saber quiénes son los proveedores de servicios permite identificar dónde se extiende el posible riesgo hacia afuera de la organización.</p>
<p>12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.</p>	<p>El reconocimiento de los proveedores de servicios demuestra su compromiso de mantener la seguridad adecuada de los datos de titulares de tarjetas que obtienen de los clientes y, por ende, los hace responsables.</p>

Requisito	Guía
<p>12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.</p>	<p>El proceso garantiza que la organización investigue minuciosamente a nivel interno todo compromiso de un proveedor de servicios; esta investigación debe incluir un análisis de los riesgos antes de establecer una relación formal con el proveedor de servicios.</p>
<p>12.8.4 Mantenga un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor de servicios.</p>	<p>Conocer el estado de cumplimiento con las PCI DSS de un proveedor de servicios ofrece mayor garantía de que cumple con los mismos requisitos a los que está sujeta una organización.</p>
<p>12.9 Implemente un plan de respuesta a incidentes. Prepárese para responder de inmediato ante un fallo en el sistema.</p>	<p>Sin un plan meticuloso de respuesta a incidentes de seguridad que las partes responsables reciban, lean y comprendan de manera adecuada, la confusión y la falta de una respuesta unificada puede provocar más tiempo de inactividad para la empresa, exposición innecesaria a los medios públicos y nuevas responsabilidades legales.</p>
<p>12.9.1 Cree el plan de respuesta a incidentes que se va a implementar en caso de fallos en el sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente:</p> <ul style="list-style-type: none"> ▪ Funciones, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago. ▪ Procedimientos específicos de respuesta a incidentes. ▪ Procedimientos de recuperación y continuidad comercial. ▪ procesos de realización de copia de seguridad de datos; ▪ Análisis de los requisitos legales para el informe de riesgos. ▪ Cobertura y respuestas de todos los componentes críticos del sistema. ▪ referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago. 	<p>El plan de respuesta a incidentes debe ser meticuloso y debe contener todos los elementos clave para permitir a su empresa responder de manera eficaz en caso de que se produzca un fallo que pueda afectar los datos de titulares de tarjetas.</p>

Requisito	Guía
<p>12.9.2 Pruebe el plan al menos una vez al año.</p>	<p>Sin una prueba adecuada, es posible que se pierdan pasos clave que limitan la exposición durante un incidente.</p>
<p>12.9.3 Designe personal especializado que se encuentre disponible permanentemente para responder a las alertas.</p>	<p>Sin un equipo de respuesta a incidentes capacitado y disponible, se puede producir un gran daño a la red y es posible que se “contaminen” datos y sistemas importantes debido al manejo no apropiado de los sistemas objetivos. Esto puede dificultar el éxito de una investigación posincidente. Si no cuenta con recursos internos disponibles, considere contratar un proveedor que le ofrezca estos servicios.</p>
<p>12.9.4 Proporcione capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad.</p>	
<p>12.9.5 Incluya alertas de sistemas de detección y prevención de intrusiones, y de monitorización de integridad de archivos.</p>	<p>Estos sistemas de monitorización están diseñados para concentrarse en los posibles riesgos para los datos. Son esenciales para tomar medidas rápidas para impedir fallos y deben incluirse en los procesos de respuesta a incidentes.</p>
<p>12.9.6 Elabore un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria.</p>	<p>La incorporación de las “lecciones aprendidas” en el plan de respuesta a incidentes ayuda a mantener el plan actualizado y capaz de reaccionar ante las nuevas emergentes y tendencias de seguridad.</p>

Guía para el requisito A.1: Requisitos de las PCI DSS adicionales para proveedores de hosting compartido

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

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

Requisito	Guía
<p>A.1 Proteger el entorno y los datos alojados de cada entidad (es decir comerciante, proveedor de servicio u otra entidad), según A.1.1 a A.1.4:</p> <p>Un proveedor de hosting debe cumplir con estos requisitos, así como también con las demás secciones correspondientes de PCI DSS.</p> <p><i>Nota: aunque posiblemente el proveedor de hosting cumpla con estos requisitos, no se garantiza el cumplimiento de la entidad que utiliza al proveedor de hosting. Cada entidad debe cumplir con las PCI DSS y validar el cumplimiento según corresponda.</i></p>	<p>El Anexo A de las PCI DSS está pensado para los proveedores de hosting compartido que desean ofrecer a los clientes de su proveedor de servicios o comerciante un entorno de hosting que cumpla con las PCI DSS. Además de todos los otros requisitos relevantes de las PCI DSS, deben cumplirse estos pasos.</p>
<p>A.1.1 Asegúrese de que cada entidad sólo lleve a cabo procesos con acceso al entorno de datos de titulares de tarjetas de la entidad.</p>	<p>Si un comerciante o un proveedor de servicios puede ejecutar sus propias aplicaciones en el servidor compartido, estas aplicaciones deberán ejecutarse con el ID de usuario del comerciante o del proveedor de servicios, en vez de como usuario privilegiado. Un usuario privilegiado tendría acceso a todos los otros entornos de datos de titulares de tarjetas de los proveedores de servicios y comerciantes y también a los datos propios.</p>

Requisito	Guía
<p>A.1.2 Restrinja el acceso y los privilegios de cada entidad para que sólo contengan el entorno de datos de titulares de tarjetas.</p>	<p>Para garantizar que el acceso y los privilegios sean limitados, de manera que un comerciante o un proveedor de servicios sólo tenga acceso a su propio entorno de datos de titulares de tarjetas, considere lo siguiente: (1) privilegios del ID de usuario del servidor web del comerciante o del proveedor de servicios; (2) permisos otorgados para leer, escribir y ejecutar los archivos; (3) permisos otorgados para escribir en binarios compartidos; (4) permisos otorgados a los archivos de registro de los proveedores de servicio y comerciantes, y (5) controles para asegurar que un comerciante o proveedor de servicios no pueda monopolizar los recursos del sistema.</p>
<p>A.1.3 Asegúrese de que los registros y las pistas de auditoría estén habilitados y sean exclusivos para el entorno de datos de titulares de tarjetas de cada entidad, así como también que cumplan con el Requisito 10 de las PCI DSS.</p>	<p>Los registros deben estar disponibles en un entorno de hosting compartido, para que los comerciantes y los proveedores de servicios puedan acceder a ellos y puedan revisar los registros específicos de su entorno de datos de titulares de tarjetas.</p>
<p>A.1.4 Habilite los procesos para proporcionar una investigación forense oportuna en caso de riesgos para un comerciante o proveedor de servicios alojado.</p>	<p>Los proveedores de hosting compartido deben tener procesos para ofrecer una respuesta rápida y simple en caso de que se necesite una investigación forense para un riesgo y deban llegar al nivel de detalle apropiado de manera que la información de un comerciante o de un proveedor de servicios en particular esté disponible.</p>

Anexo A: Normas de seguridad de datos de la PCI: documentos relacionados

Los siguientes documentos fueron creados para ayudar a los comerciantes y a los proveedores de servicios a comprender las Normas de seguridad de datos de la PCI y las responsabilidades y los requisitos de cumplimiento.

Documento	Destinatarios
<i>Requisitos de normas de seguridad de datos de la PCI y procedimientos de evaluación de seguridad</i>	Todos los comerciantes y proveedores de servicios
<i>Exploración de PCI DSS: Comprensión del objetivo de los requisitos</i>	Todos los comerciantes y proveedores de servicios
<i>Normas de seguridad de datos de la PCI: Instrucciones y directrices del cuestionario de autoevaluación</i>	Todos los comerciantes y proveedores de servicios
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación A</i>	Comerciantes ¹⁰
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación B</i>	Comerciantes ¹⁰
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación C</i>	Comerciantes ¹⁰
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación D</i>	Comerciantes ¹⁰ y todos los proveedores de servicios
<i>Glosario de términos, abreviaturas y acrónimos de las PCI DSS</i>	Todos los comerciantes y proveedores de servicios

¹⁰ Para determinar el Cuestionario de Autoevaluación apropiado, consulte las *Normas de seguridad de datos de la PCI: Instrucciones y directrices del cuestionario de autoevaluación*, "Selección del SAC y de la declaración que mejor se adapta a su organización".