



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

Cuestionario de autoevaluación C y Declaración de cumplimiento

**Aplicación de pago con conexión a Internet,
almacenamiento no electrónico de datos de
titulares de tarjetas**

Versión 1.2

Octubre de 2008

Modificaciones realizadas a los documentos

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

Índice

Modificaciones realizadas a los documentos.....	i
Normas de seguridad de datos de la PCI: documentos relacionados	iii
Antes de comenzar	iv
Complete el Cuestionario de Autoevaluación	iv
Cumplimiento de las DSS de la PCI: pasos de cumplimiento	iv
Guía para la no aplicabilidad y exclusión de ciertos requisitos específicos	v
Declaración de cumplimiento, SAC C	1
Cuestionario de autoevaluación C.....	5
Desarrollar y mantener una red segura	5
<i>Requisito 1: Instale y mantenga una configuración de firewall para proteger los datos</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>5</i>
Proteja los datos del titular de la tarjeta	6
<i>Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados</i>	<i>6</i>
<i>Requisito 4: Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.....</i>	<i>7</i>
Desarrolle un programa de administración de vulnerabilidad	8
<i>Requisito 5: Utilice y actualice regularmente el software o los programas antivirus</i>	<i>8</i>
<i>Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.....</i>	<i>8</i>
Implemente medidas sólidas de control de acceso	9
<i>Requisito 7: Restrinja el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa</i>	<i>9</i>
<i>Requisito 8: Asigne una ID única a cada persona que tenga acceso a equipos.....</i>	<i>9</i>
<i>Requisito 9: Limite el acceso físico a los datos del titular de la tarjeta.....</i>	<i>9</i>
Supervise y pruebe las redes con regularidad.....	10
<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>10</i>
<i>Requisito 11: Pruebe los sistemas y procesos de seguridad regularmente.....</i>	<i>10</i>
Mantenga una política de seguridad de información.....	11
<i>Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas.....</i>	<i>11</i>
Anexo A: (no se usa)	12
Anexo B: Controles de compensación.....	13
Anexo C: Hoja de trabajo de controles de compensación	14
Hoja de trabajo de controles de compensación—Ejemplo completo	15
Anexo D: Explicación de no aplicabilidad	16

Normas de seguridad de datos de la PCI: documentos relacionados

Los siguientes documentos se crearon para ayudar a los comerciantes y a los proveedores de servicios a comprender las Normas de seguridad de datos de la PCI y el Cuestionario de Autoevaluación de las PCI DSS.

Documento	Destinatarios
<i>Requisitos de normas de seguridad de datos de la PCI y procedimientos de evaluación de seguridad</i>	Todos los comerciantes y los proveedores de servicios
<i>Exploración de PCI DSS: Comprensión del objetivo de los requisitos</i>	Todos los comerciantes y los proveedores de servicios
<i>Normas de seguridad de datos de la PCI: Instrucciones y directrices de autoevaluación</i>	Todos los comerciantes y los proveedores de servicios
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación A</i>	Comerciantes ¹
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación B</i>	Comerciantes ¹
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación C</i>	Comerciantes ¹
<i>Normas de seguridad de datos de la PCI: Declaración y cuestionario de autoevaluación D</i>	Comerciantes ¹ y todos los proveedores de servicios
<i>Glosario de términos, abreviaturas y acrónimos de las Normas de Seguridad de Datos para las Aplicaciones de Pago y las Normas de seguridad de datos de la PCI</i>	Todos los comerciantes y los proveedores de servicios

¹ Para determinar el Cuestionario de Autoevaluación apropiado, consulte las *Normas de seguridad de datos de la PCI: Instrucciones y directrices de autoevaluación*, “Selección del SAC y de la declaración que mejor se adapta a su organización”.

Antes de comenzar

Complete el Cuestionario de Autoevaluación

El SAC C ha sido diseñado para tratar los requisitos aplicables a comerciantes que procesan datos de titulares de tarjetas a través de aplicaciones de pago (por ejemplo, sistemas de POS) conectados a Internet (conexión de alta velocidad, DSL, cable módem, etc.), pero que no almacenan datos de titulares de tarjetas en ningún sistema informático. Estas aplicaciones de pago están conectadas a Internet porque:

1. La aplicación de pago se encuentra en una computadora personal conectada a Internet, o
2. La aplicación de pago está conectada a Internet para transmitir datos de titulares de tarjetas.

Estos comerciantes se definen como Validación del SAC Tipo 4, según se define aquí y en las *Instrucciones y directrices del cuestionario de autoevaluación de las PCI DSS*. Los comerciantes de Validación Tipo 4 procesan los datos de titulares de tarjetas a través de máquinas de POS conectadas a Internet, no almacenan datos de titulares de tarjetas en ningún sistema informático y pueden ser comerciantes con instalaciones físicas (tarjeta presente) o con pedido por correo/teléfono o comercio electrónico. Estos comerciantes deben validar el cumplimiento completando el SAC C y la Declaración de cumplimiento asociada, que confirma:

- Que su empresa tiene un sistema de aplicación de pago y una conexión a Internet en el mismo dispositivo;
- Que su dispositivo de Internet/aplicación de pago no está conectado a ningún otro sistema dentro de su entorno;
- Que su empresa conserva sólo informes en papel o copias en papel de recibos;
- Que su empresa no almacena datos de titulares de tarjetas en formato electrónico; y
- Que el proveedor de la aplicación de pago de su empresa usa técnicas seguras para ofrecer asistencia remota para su sistema de pago.

Cada sección de este cuestionario se concentra en un área específica de seguridad, en base a los requisitos de las Normas de seguridad de datos de la PCI.

Cumplimiento de las DSS de la PCI: pasos de cumplimiento

1. Complete el Cuestionario de Autoevaluación (SAC C) según las *Instrucciones y directrices del cuestionario de autoevaluación*.
2. Complete un análisis de vulnerabilidades aprobado con un Proveedor Aprobado de Escaneo (ASV) de PCI SSC y solicite pruebas de un análisis aprobado al ASV.
3. Complete la Declaración de cumplimiento en su totalidad.
4. Presente el SAC, las pruebas del análisis aprobado y la Declaración de cumplimiento junto con todo otro documento solicitado al adquirente.

Guía para la no aplicabilidad y exclusión de ciertos requisitos específicos

Exclusión: Si se le solicita que responda el SAC para validar su cumplimiento de las PCI DSS, puede considerarse la siguiente excepción. Consulte “No aplicabilidad” a continuación para obtener la respuesta del SAC apropiada.

- Las preguntas específicas del sistema inalámbrico sólo deben responderse si el sistema inalámbrico está incorporado en su red (por ejemplo, el Requisito 2.1.1). Tenga en cuenta que el Requisito 11.1 (uso del analizador inalámbrico) debe responderse incluso si el sistema inalámbrico no está incorporado en su red, ya que el analizador detecta cualquier dispositivo no autorizado o pícaro que se haya incorporado sin que el comerciante esté al tanto.

No aplicabilidad: Éste y cualquier otro requisito que considere que no corresponde a su entorno debe marcarse como “N/C” en la columna “Especial” del SAC. Según el caso, complete la hoja de trabajo “Explicación de no aplicabilidad” en el Anexo para cada entrada “N/C”.

Declaración de cumplimiento, SAC C

Instrucciones para la presentación

El comerciante debe completar esta Declaración de cumplimiento como su declaración del estado de cumplimiento de los Requisitos de las *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)* y los *procedimientos de evaluación de seguridad*. Complete todas las secciones que corresponda y consulte las instrucciones de presentación en Pasos para completar el cumplimiento de las PCI DSS en este documento.

Parte 1. Información de la empresa sobre el Asesor de Seguridad Certificado (si corresponde)

Nombre de la empresa:				
Nombre de contacto del QSA principal:	Cargo:			
N.º de teléfono:	Dirección de correo electrónico:			
Dirección comercial:	Ciudad:			
Estado/Provincia:	País:	Código postal:		
URL:				

Parte 2. Información sobre la organización del comerciante

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

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

- Comercio minorista
 Telecomunicaciones
 Tienda de comestibles y supermercados
 Petróleo
 Comercio electrónico
 Pedidos por correo/teléfono
 Otros (especifique):

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

Parte 2b. Relaciones

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

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

Parte 2c. Procesamiento de transacciones

Aplicación de pago en uso:

Versión de la aplicación de pago:

Parte 2d. Elegibilidad para completar el SAC C

El comerciante certifica la elegibilidad para completar esta versión abreviada del Cuestionario de Autoevaluación porque:

- El comerciante tiene un sistema de aplicación de pago y una conexión a Internet o a una red pública en el mismo dispositivo;
- El dispositivo de Internet/sistema de aplicación de pago no está conectado a ningún otro sistema dentro del entorno comercial;
- El comerciante no almacena datos de titulares de tarjetas en formato electrónico;
- Si un comerciante no almacena datos de titulares de tarjetas, esos datos sólo se encuentran en informes en papel o en copias en papel de recibos y no se reciben electrónicamente; y
- El proveedor del software de la aplicación de pago del comerciante usa técnicas seguras para ofrecer asistencia remota para el sistema de aplicación de pago del comerciante.

Parte 3. Validación de las PCI DSS

En base a los resultados observados en el SAC C con fecha del *(fecha en la que se completó)*, *(Nombre de la empresa)* afirma el siguiente estado de cumplimiento (marque uno):

- Conforme:** Todas las secciones del SAC de la PCI están completas y se han respondido todas las preguntas con "Sí", lo que tiene como resultado una calificación general de **CONFORME**; además, un Proveedor Aprobado de Escaneo de PCI SSC ha completado un análisis aprobado; así *(Nombre de la empresa)* ha demostrado el cumplimiento total de las PCI DSS.
- No conforme:** No todas las secciones del SAC de la PCI están completas y algunas preguntas se han respondido con "No", lo que tiene como resultado una calificación general de **NO CONFORME** o un Proveedor Aprobado de Escaneo de PCI SSC no ha completado un análisis aprobado; así *(Nombre de la empresa)* no ha demostrado el cumplimiento total de las PCI DSS.

Fecha objetivo para el cumplimiento:

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

Parte 3a. Confirmación del estado de cumplimiento

Confirmación del comerciante:

<input type="checkbox"/>	El Cuestionario de autoevaluación C de las PCI DSS, Versión (<i>versión del SAC</i>), se completó según las instrucciones del mismo.
<input type="checkbox"/>	Toda la información que aparece dentro del SAC antes mencionado y en esta declaración muestran los resultados de mi evaluación de manera equitativa en todos sus aspectos sustanciales.
<input type="checkbox"/>	He confirmado con mi proveedor de la aplicación de pago que mi sistema de aplicación de pago no almacena los datos de autenticación confidenciales después de la autorización.
<input type="checkbox"/>	He leído las PCI DSS y reconozco que debo cumplir plenamente con las PCI DSS en todo momento.
<input type="checkbox"/>	No existe evidencia de almacenamiento de datos ² de banda magnética (es decir, ninguna pista), datos de CAV2, CVC2, CID, o CVV2 ³ , ni datos de PIN ⁴ después de encontrarse la autorización de la transacción en TODOS los sistemas revisados durante la presente evaluación.

Parte 3b. Reconocimiento del comerciante

<i>Firma del Oficial Ejecutivo del comerciante</i> ↑	<i>Fecha</i> ↑
<i>Nombre del Oficial Ejecutivo del comerciante</i> ↑	<i>Cargo</i> ↑

Empresa representada ↑

² Datos codificados en la banda magnética que se utilizan para realizar la autorización durante una transacción con tarjeta presente. Es posible que las entidades no retengan todos los datos de banda magnética después de la autorización de la transacción. Los únicos elementos de datos de pistas que se pueden retener son: el número de cuenta, la fecha de vencimiento y el nombre.

³ 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).

⁴ El número de identificación personal introducido por el titular de la tarjeta durante una transacción con tarjeta presente y/o el bloqueo del PIN cifrado presente dentro del mensaje de la transacción.

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

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

Requisito de las PCI DSS	Descripción del requisito	Estado de cumplimiento (Seleccione uno)		Fecha de la recuperación y acciones (si el estado de cumplimiento es "NO")
		SÍ	NO	
1	Instale y mantenga una configuración de firewall para proteger los datos de los titulares de las tarjetas	<input type="checkbox"/>	<input type="checkbox"/>	
2	No utilice los valores predeterminados que ofrece el proveedor para las contraseñas del sistema u otros parámetros de seguridad	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteja los datos del titular de la tarjeta que fueron almacenados	<input type="checkbox"/>	<input type="checkbox"/>	
4	Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.	<input type="checkbox"/>	<input type="checkbox"/>	
5	Utilice un software antivirus y actualícelo regularmente	<input type="checkbox"/>	<input type="checkbox"/>	
6	Desarrolle y mantenga sistemas y aplicaciones seguras	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrinja el acceso a datos de titulares de tarjetas sólo a la necesidad de conocimiento de la empresa	<input type="checkbox"/>	<input type="checkbox"/>	
8	Asigne una ID única a cada persona que tenga acceso a equipos	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limite el acceso físico a los datos del titular de la tarjeta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Pruebe los sistemas y procesos de seguridad regularmente	<input type="checkbox"/>	<input type="checkbox"/>	
12	Mantenga una política que aborde la seguridad de la información	<input type="checkbox"/>	<input type="checkbox"/>	

Cuestionario de autoevaluación C

Fecha en la que se completó:

Desarrollar y mantener una red segura

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

Pregunta	Respuesta	Sí	No	Especial*
1.2 ¿La configuración del firewall restringe las conexiones entre redes no confiables y todo sistema del entorno de datos de titulares de tarjeta de la siguiente manera?: <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>		<input type="checkbox"/>	<input type="checkbox"/>	
1.3 ¿La configuración de firewall prohíbe el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pregunta	Respuesta	Sí	No	Especial*
2.1 ¿Siempre se cambian los valores predeterminados de los proveedores antes de instalar un sistema en la red? <i>Por ejemplo, contraseñas, las cadenas comunitarias de protocolo simple de administración de red (SNMP) y eliminación de cuentas innecesarias.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1 (a) ¿Los valores predeterminados* para los entornos inalámbricos están conectados al entorno de datos de titulares de tarjetas o transmiten los datos de titulares de tarjetas que se cambian antes de instalar un sistema inalámbrico? <i>* Estos valores predeterminados de entornos inalámbricos incluyen, a modo de ejemplo, claves de criptografía inalámbricas predeterminadas, contraseñas y cadenas comunitarias SNMP.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
(b) ¿Está habilitada la configuración de seguridad de los dispositivos inalámbricos para la tecnología de cifrado de la autenticación y transmisión?		<input type="checkbox"/>	<input type="checkbox"/>	
2.3 ¿Está cifrado el acceso administrativo que no sea de consola? <i>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.</i>		<input type="checkbox"/>	<input type="checkbox"/>	

* "No aplicable" (N/A) o "Controles de compensación utilizados". Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

Proteja los datos del titular de la tarjeta

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

Pregunta	Respuesta	Sí	No	Especial*
3.2 ¿Todos los sistemas se adhieren a los siguientes requisitos con respecto al almacenamiento de datos confidenciales de autenticación después de la autorización (incluso si están cifrados)?		<input type="checkbox"/>	<input type="checkbox"/>	
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. <i>En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:</i> <ul style="list-style-type: none"> ▪ El nombre del titular de la tarjeta, ▪ Número de cuenta principal (PAN). ▪ Fecha de vencimiento. ▪ Código de servicio. <i>Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio. NUNCA almacene el código de verificación de la tarjeta, el valor ni los elementos de datos del valor de verificación del PIN.</i> <i>Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
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. <i>Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.3 No almacene el número de identificación personal (PIN) ni el bloqueo del PIN cifrado.		<input type="checkbox"/>	<input type="checkbox"/>	
3.3 ¿Se oculta el PAN cuando aparece? (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá). <i>Notas:</i> <ul style="list-style-type: none"> ▪ Este requisito no se aplica a trabajadores y a otras partes que posean una necesidad específica de conocer el PAN completo; ▪ Este requisito no reemplaza los requisitos más estrictos que fueron implementados y que aparecen en los datos del titular de la tarjeta (por ejemplo, los recibos de puntos de venta [POS]). 		<input type="checkbox"/>	<input type="checkbox"/>	

* “No aplicable” (N/A) o “Controles de compensación utilizados”. Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

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

	Pregunta	Respuesta	Sí	No	Especial*
4.1	<p>¿Se utilizan 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>Algunos ejemplos de redes públicas abiertas que se encuentran dentro del ámbito de aplicación de las PCI DSS son Internet, tecnologías inalámbricas, el sistema global de comunicaciones móviles (GSM) y el servicio de radio paquete general (GPRS).</i></p> <p><i>Nota: Si ha implementado tecnología inalámbrica en su entorno, debe estar al tanto de lo siguiente:</i></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> 		<input type="checkbox"/>	<input type="checkbox"/>	
4.2	<p>¿Se han implementado políticas, procedimientos y prácticas para impedir el envío de PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea o el chat)?</p>		<input type="checkbox"/>	<input type="checkbox"/>	

* “No aplicable” (N/A) o “Controles de compensación utilizados”. Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

Desarrolle un programa de administración de vulnerabilidad

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

	Pregunta	Respuesta	Sí	No	Especial*
5.1	¿Se ha implementado un software antivirus en todos los sistemas, en especial, computadoras personales y servidores, comúnmente afectados por software malicioso?		<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	¿Todos los programas antivirus son capaces de detectar y eliminar todos los tipos conocidos de software malicioso y de proteger los sistemas contra éstos?		<input type="checkbox"/>	<input type="checkbox"/>	
5.2	¿Todos los mecanismos antivirus son actuales, están en funcionamiento y son capaces de generar registros de auditoría?		<input type="checkbox"/>	<input type="checkbox"/>	

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

	Pregunta	Respuesta	Sí	No	Especial*
6.1	(a) ¿Todos los componentes de sistemas y software cuentan con los parches de seguridad más recientes proporcionados por los proveedores?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Los parches importantes de seguridad se instalan dentro de un plazo de un mes de su lanzamiento? <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>		<input type="checkbox"/>	<input type="checkbox"/>	

* “No aplicable” (N/A) o “Controles de compensación utilizados”. Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

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

Pregunta	Respuesta	Sí	No	Especial*
7.1 (a) ¿Se limita el acceso a los componentes del sistema y a los datos de titulares de tarjetas a aquellos individuos cuyas tareas necesitan de ese acceso?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pregunta	Respuesta	Sí	No	Especial*
8.5.6 ¿Las cuentas que utilizan los proveedores para el mantenimiento remoto se activan únicamente durante el período necesario?		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pregunta	Respuesta	Sí	No	Especial*
9.6 ¿Se resguardan de forma física todos los papeles y dispositivos electrónicos que contienen datos de titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7 (a) ¿Se lleva un control estricto sobre la distribución interna o externa de todo tipo de medios que contiene datos de titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
(b) ¿Los controles incluyen lo siguiente?				
9.7.1 ¿Los medios se clasifican de manera que se puedan identificar como confidenciales?		<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2 ¿Los medios se envían por correo seguro o por otro método de envío que se pueda rastrear con precisión?		<input type="checkbox"/>	<input type="checkbox"/>	
9.8 ¿Se han implementado procesos y procedimientos para garantizar la aprobación de la gerencia antes de mover cualquier medio que contenga datos de titulares de tarjetas de un área segura (especialmente cuando los medios se distribuyen a personas)?		<input type="checkbox"/>	<input type="checkbox"/>	
9.9 ¿Se lleva un control estricto sobre el almacenamiento y la accesibilidad de los medios que contengan datos de titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10 ¿Se destruyen los medios que contienen datos de titulares de tarjetas cuando ya no son necesarios para la empresa o por motivos legales? La destrucción debe ser de la siguiente manera:		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1 ¿Los materiales de copias en papel se cortan en tiras, se incineran o se hacen pasta para que los datos de titulares de tarjetas no puedan reconstruirse?		<input type="checkbox"/>	<input type="checkbox"/>	

* “No aplicable” (N/A) o “Controles de compensación utilizados”. Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

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

Pregunta	Respuesta	Sí	No	Especial*
No hay preguntas que correspondan al SAC C.				

Requisito 11: Pruebe los sistemas y procesos de seguridad regularmente

Pregunta	Respuesta	Sí	No	Especial*
11.1 ¿Se realizan 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?		<input type="checkbox"/>	<input type="checkbox"/>	
11.2 ¿Se realizan 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)? <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>		<input type="checkbox"/>	<input type="checkbox"/>	

* “No aplicable” (N/A) o “Controles de compensación utilizados”. Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

Mantenga una política de seguridad de información

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

Pregunta	Respuesta	Sí	No	Especial*
12.1 ¿Se ha establecido, publicado, mantenido y diseminado una política de seguridad? ¿Cumple con lo siguiente?:		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.3 ¿Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno?		<input type="checkbox"/>	<input type="checkbox"/>	
12.3 (a) ¿Se desarrollan 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?		<input type="checkbox"/>	<input type="checkbox"/>	
12.4 ¿Las políticas y los procedimientos de seguridad definen claramente las responsabilidades de seguridad de la información de todos los empleados y contratistas?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5 ¿Se asignan las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo?				
12.5.3 ¿Se establecen, documentan y distribuyen procedimientos de respuesta ante incidentes de seguridad y escalación para garantizar un manejo oportuno y efectivo de todas las situaciones?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6 ¿Se ha implementado 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?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8 Si se comparten los datos de titulares de tarjetas con proveedores de servicios, ¿se mantienen e implementan políticas y procedimientos para administrar proveedores de servicios? ¿las políticas y los procedimientos incluyen lo siguiente?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1 Se mantiene una lista de proveedores de servicios.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2 Se mantiene un acuerdo escrito que incluye 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.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3 Existe un proceso para comprometer a los proveedores de servicios que incluye una auditoría de compra adecuada previa al compromiso.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4 Se mantiene un programa para supervisar el estado de cumplimiento de las PCI DSS de los proveedores de servicios.		<input type="checkbox"/>	<input type="checkbox"/>	

* “No aplicable” (N/A) o “Controles de compensación utilizados”. Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo de explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.

Anexo A: (no se usa)

Esta página se dejó en blanco de manera intencional

Anexo B: Controles de compensación

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

Los controles de compensación deben cumplir con los siguientes criterios:

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

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

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

- a) Los requisitos de las PCI DSS NO SE PUEDEN considerar controles de compensación si ya fueron requisito para el elemento en revisión. Por ejemplo, las contraseñas para el acceso administrativo sin consola se deben enviar cifradas para mitigar el riesgo de que se intercepten contraseñas administrativas de texto claro. Una entidad no puede utilizar otros requisitos de contraseña de las PCI DSS (bloqueo de intrusos, contraseñas complejas, etc.) para compensar la falta de contraseñas cifradas, puesto que esos otros requisitos de contraseña no mitigan el riesgo de que se intercepten las contraseñas de texto claro. Además, los demás controles de contraseña ya son requisitos de las PCI DSS para el elemento en revisión (contraseñas).
 - b) Los requisitos de las PCI DSS SE PUEDEN considerar controles de compensación si se requieren para otra área, pero no son requisito para el elemento en revisión. Por ejemplo, la autenticación de dos factores es un requisito de las PCI DSS para el acceso remoto. La autenticación de dos factores *desde la red interna* también se puede considerar un control de compensación para el acceso administrativo sin consola cuando no se puede admitir la transmisión de contraseñas cifradas. La autenticación de dos factores posiblemente sea un control de compensación aceptable si; (1) cumple con el propósito del requisito original al abordar el riesgo de que se intercepten las contraseñas administrativa de texto claro y (2) está adecuadamente configurada y en un entorno seguro.
 - c) Los requisitos existentes de la PCI DSS se pueden combinar con nuevos controles para convertirse en un control de compensación. Por ejemplo, si una empresa no puede dejar ilegibles los datos de los titulares de tarjetas según el requisito 3.4 (por ejemplo, mediante cifrado), un control de compensación podría constar de un dispositivo o combinación de dispositivos, aplicaciones y controles que aborden lo siguiente: (1) segmentación interna de la red; (2) filtrado de dirección IP o MAC y (3) autenticación de dos factores desde la red interna.
4. Sea cuidadoso con el riesgo adicional que impone la no adhesión al requisito de las PCI DSS

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

Anexo C: Hoja de trabajo de controles de compensación

Utilice esta hoja de trabajo para definir los controles de compensación para cualquier requisito en el que se marcó “Sí” y se mencionaron controles de compensación en la columna “Especial”.

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

Número de requisito y definición:

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

Hoja de trabajo de controles de compensación—Ejemplo completo

Utilice esta hoja de trabajo para definir los controles de compensación para cualquier requisito en el que se marcó “Sí” y se mencionaron controles de compensación en la columna “Especial”.

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

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

