



Cuestionario de autoevaluación B y Declaración de cumplimiento de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI)

**Máquinas de impresión o terminales
independientes con discado externo sin
almacenamiento electrónico de los datos de los
titulares de tarjetas**

Versión 1.2

Octubre 2008

Modificaciones realizadas a los documentos

Fecha	Versión	Descripción
1.º 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
Cómo completar el Cuestionario de autoevaluación	iv
Cumplimiento de las DSS de la PCI: pasos de cumplimiento	iv
Guía para la no aplicabilidad de ciertos requisitos específicos	iv
Declaración de cumplimiento, SAQ B	1
Cuestionario de autoevaluación B	5
Proteja los datos del titular de la tarjeta	5
<i>Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados</i>	<i>5</i>
<i>Requisito 4: Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.</i>	<i>6</i>
Implemente medidas sólidas de control de acceso	7
<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>7</i>
<i>Requisito 9: Limite el acceso físico a los datos del titular de la tarjeta</i>	<i>7</i>
Mantenga una política de seguridad de información	8
<i>Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas.</i>	<i>8</i>
Anexo A: (no utilizado)	9
Anexo B: Controles de compensación	10
Anexo C: Hoja de trabajo de controles de compensación	11
Hoja de trabajo de controles de compensación – Ejemplo completo	12
Anexo D: Explicaciones de no aplicabilidad	13

Normas de seguridad de datos de la PCI: documentos relacionados

Los siguientes documentos han sido creados para ayudar a los comerciantes y proveedores de servicios a entender las normas de seguridad de la PCI y el cuestionario de autoevaluación de las normas 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 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 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 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 de la PCI y normas de seguridad de datos para las aplicaciones de pago</i>	Todos los comerciantes y 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

Cómo completar el Cuestionario de autoevaluación

El cuestionario SAQ B ha sido desarrollado para responder a los requisitos de comerciantes que procesan datos de los titulares de tarjetas mediante máquinas de impresión o terminales independientes con discado externo.

Estos comerciantes se definen como comerciantes del Tipo de validación de SAQ 2 y 3, tanto en este documento como en *Instrucciones y directrices para completar el cuestionario de autoevaluación de las normas PCI DSS*. Los comerciantes del Tipo de validación de SAQ 2 procesan los datos de los titulares de tarjetas mediante máquinas de impresión. Los comerciantes del Tipo de validación de SAQ 3 procesan los datos de los titulares de tarjetas mediante terminales independientes con discado externo. Los dos tipos de comerciantes pueden ser comerciantes con instalaciones físicas, donde la tarjeta es visible, o comerciantes que toman pedidos mediante medios electrónicos (e-commerce) o por correo o teléfono, donde la tarjeta no es visible. Deben validar el cumplimiento completando el SAQ B y la Declaración de cumplimiento correspondiente, para confirmar que:

Para el Tipo de validación 2:

- Su empresa utiliza solamente máquinas de impresión.
- Su empresa no transfiere los datos de los titulares de tarjetas por teléfono o Internet.
- Su empresa conserva solamente informes en papel o copias en papel de recibos
- Su empresa no almacena los datos de los titulares de tarjetas en formato electrónico

Para el Tipo de validación 3:

- Su empresa utiliza solamente terminales independientes con discado externo (conectadas al procesador mediante la línea telefónica).
- Las terminales independientes con discado externo no están conectadas a ningún otro sistema ni a Internet.
- Su empresa conserva solamente informes en papel o copias en papel de recibos
- Su empresa no almacena los datos de los titulares de tarjetas en formato electrónico.

Cada sección del cuestionario está orientada a un área específica de seguridad, según los requisitos estipulados en 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 (SAQ B) según las *Instrucciones y directrices para completar el cuestionario de autoevaluación de las normas PCI DSS*.
2. Complete la Declaración de cumplimiento en su totalidad.
3. Presente al adquirente el cuestionario SAQ y la Declaración de cumplimiento junto con cualquier otro documento solicitado.

Guía para la no aplicabilidad de ciertos requisitos específicos

No aplicabilidad: Los requisitos que se consideren no aplicable a su entorno deben indicarse escribiendo “N/A” en la columna “Especial” del SAQ. Asimismo, sírvase completar la hoja de trabajo para “Explicaciones de no aplicabilidad” que se encuentra en el anexo de cada entrada.

Declaración de cumplimiento, SAQ B

Instrucciones para la presentación

El comerciante debe completar esta Declaración de cumplimiento para manifestar su estado de cumplimiento con los *Requisitos y Procedimientos de Evaluación de Seguridad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)*. Complete todas las secciones aplicables y consulte las instrucciones para presentar esta declaración en la sección "Cumplimiento con las normas PCI DSS: pasos para completar el proceso", incluida en este documento.

Parte 1. Información sobre la empresa del 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 las normas PCI DSS:

Parte 2b. Relaciones

¿Su empresa tiene relación con uno o más proveedores de servicios externos (por ejemplo, empresas de puertos 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 cuestionario SAQ B

El comerciante certifica su elegibilidad para completar esta versión abreviada del Cuestionario de autoevaluación porque:

- | | | |
|--------------------------|-----------|--|
| <input type="checkbox"/> | A. | El comerciante utiliza solamente máquinas de impresión para imprimir la información relativa a la tarjeta de pago del cliente y no transfiere datos de los titulares de tarjetas por teléfono o Internet. |
| | B. | El comerciante utiliza terminales independientes con marcado externo, que no están conectadas a Internet ni a ningún otro sistema dentro del entorno del comerciante. |
| <input type="checkbox"/> | | El comerciante no almacena los datos de los titulares de tarjetas en formato electrónico. |
| <input type="checkbox"/> | | Debido a que el comerciante no almacena los datos de los titulares de tarjetas, esos datos se conservan solamente como informes en papel o copias de recibos en papel, y no son recibidos por medios electrónicos. |

Parte 3. Validación de las PCI DSS

Según los resultados observados en el cuestionario SAQ B con fecha (*fecha de compleción*), (*Nombre de la empresa del comerciante*) declara que el estado de cumplimiento es el siguiente (marque una opción):

- Conforme:** Se han completado todas las secciones del cuestionario SAQ de la PCI y la respuesta a todas las preguntas es "Sí", lo que da como resultado una clasificación general de **CUMPLIMIENTO**. Por tanto, (*Nombre de la empresa del comerciante*) ha demostrado un total cumplimiento con las Normas de seguridad de datos de la PCI.
- No conforme:** Se han completado todas las secciones del cuestionario SAQ de la PCI y algunas respuestas obtuvieron "No" como respuesta, lo que da como resultado una clasificación general de **INCUMPLIMIENTO**. Por tanto, (*Nombre de la empresa del comerciante*) no ha demostrado un total cumplimiento con las Normas de seguridad de datos de la PCI.

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

El comerciante confirma que:

<input type="checkbox"/>	El Cuestionario de autoevaluación B de las PCI DSS, versión (<i>versión del SAQ</i>), se completó siguiendo las instrucciones dadas.
<input type="checkbox"/>	Toda la información que aparece en el cuestionario antes mencionado y en esta declaración muestran los resultados de la evaluación de manera equitativa.
<input type="checkbox"/>	Le he confirmado a mi proveedor de aplicaciones de pago que mi sistema de pago no almacena datos de autenticación confidenciales después de otorgada la autorización.
<input type="checkbox"/>	He leído las normas PCI DSS y reconozco que debo cumplirlas 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. Confirmación del comerciante

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

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 adquiriente o la(s) marca(s) de pago antes de completar la Parte 4, ya que no todas las marcas de pago necesitan esta sección.*

Requisitos de las PCI DSS	Descripción del requisito	Estado de cumplimiento (Seleccione uno)		Fecha de la reparación y acciones (si el estado de cumplimiento es “NO”)
		SÍ	NO	
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"/>	
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"/>	
9	Limite el acceso físico a los datos del titular de la tarjeta	<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 B

Fecha de cumplimiento:

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 ¿Se adhieren todos los sistemas a los siguientes requisitos en relación con el almacenamiento de datos confidenciales de autenticación después de recibir la autorización (aun cuando estén 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"/>	

* “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.

Pregunta		Respuesta:	<u>Sí</u>	<u>No</u>	<u>Especial*</u>
3.3	<p>¿Se enmascara el PAN cuando se muestra? 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> 		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pregunta		Respuesta:	<u>Sí</u>	<u>No</u>	<u>Especial*</u>
4.2	<p>¿Existen políticas, procedimientos y prácticas establecidos para evitar que se envíen 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.

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*
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7.1 ¿Se encuentra limitado el acceso a los componentes del sistema y a los datos de los titulares de tarjetas a aquellos individuos cuyas tareas necesitan de ese acceso?		<input type="checkbox"/>	<input type="checkbox"/>	<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*
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.6 ¿Están todos los papeles y dispositivos electrónicos que contienen datos de los titulares de tarjetas resguardados de forma física?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.7 (a) ¿Lleva un control estricto sobre la distribución interna o externa de cualquier tipo de medios que contengan datos de los titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
(b) ¿Incluyen los controles lo siguiente?						
9.7.1 ¿Se encuentran los medios clasificados de manera que se puedan identificar como confidenciales?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.7.2 ¿Se envía medios por correo seguro u otro método de envío que se pueda rastrear con precisión?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.8 ¿Existen procesos y procedimientos establecidos para asegurar que se obtenga aprobación de la administración antes de trasladar cualquier medio con los datos de titulares de tarjetas desde un área segura (especialmente cuando se los distribuye a personas)?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.9 ¿Se mantiene un control estricto sobre el almacenamiento y accesibilidad de los medios que contienen datos de los titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.10 ¿Se destruyen los medios que contengan datos de titulares de tarjetas cuando ya no sean necesarios para la empresa o por motivos legales? La destrucción debe realizarse de la siguiente manera:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
9.10.1 ¿Se pasan los materiales de copias en papel por una trituradora que corte en zig zag, se incineran o se hacen pasta de modo que sea imposible reconstruirlos?		<input type="checkbox"/>	<input type="checkbox"/>	<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	¿Existe una política de seguridad establecida, publicada, mantenida y distribuida, que incluye y logra 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 encuentran las siguientes responsabilidades de gestión de seguridad informática asignadas a una persona o a un equipo?				
12.5.3	¿Se establecen, documentan y distribuyen los procedimientos de respuesta ante incidentes de seguridad y escalamiento para garantizar un manejo oportuno y efectivo de todas las situaciones?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6	¿Se encuentra 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 los titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8	Si los datos de los titulares de tarjetas se comparten con proveedores de servicios, ¿se mantienen e implementan políticas y procedimientos a los fines de administrar proveedores de servicios? ¿Incluyen estos procedimientos y políticas lo siguiente?		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.1	La conservación de una lista de proveedores de servicios.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.2	Un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de los titulares de tarjetas que ellos tienen en su poder.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.3	La existencia de un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.		<input type="checkbox"/>	<input type="checkbox"/>	
12.8.4	El mantenimiento de un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor 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 utilizado)

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>

