



**Normas de Seguridad de Datos de la
Industria de Tarjetas de Pago (PCI)
Cuestionario de autoevaluación D
y declaración de cumplimiento**

**Dirigido a todo otro comerciante y a todos los
proveedores de servicios que cumplan con los
requisitos para realizar un SAQ**

Versión 1.2

Octubre de 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 PCI DSS: pasos de conclusión.....	v
Guía para la no aplicabilidad y exclusión de ciertos requisitos específicos	v
Declaración de cumplimiento, SAQ D: versión para el comerciante.....	1
Declaración de cumplimiento, SAQ D: versión para proveedor de servicios.....	5
Cuestionario de autoevaluación D.....	9
Desarrollar y mantener una red segura	9
<i>Requisito 1: Instale y mantenga una configuración de firewall para proteger los datos</i>	<i>9</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>11</i>
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>15</i>
Desarrolle un programa de administración de vulnerabilidad	17
<i>Requisito 5: Utilice y actualice regularmente el software o los programas antivirus</i>	<i>17</i>
<i>Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.....</i>	<i>17</i>
Implemente medidas sólidas de control de acceso	20
<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>20</i>
<i>Requisito 8: Asigne una ID única a cada persona que tenga acceso a computadoras.....</i>	<i>20</i>
<i>Requisito 9: Limite el acceso físico a los datos del titular de la tarjeta.....</i>	<i>22</i>
Supervise y pruebe las redes con regularidad.....	25
<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>25</i>
<i>Requisito 11: Pruebe los sistemas y procesos de seguridad regularmente.....</i>	<i>26</i>
Mantenga una política de seguridad de información	28
<i>Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas.....</i>	<i>28</i>
Anexo A: Requisitos de las PCI DSS adicionales para proveedores de hosting compartido.....	31
<i>Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de los titulares de tarjetas.....</i>	<i>31</i>
Anexo B: Controles de compensación.....	32
Anexo C: Hoja de trabajo de controles de compensación	33
Hoja de trabajo de controles de compensación – Ejemplo completo.....	34
Anexo D: Explicación de no aplicabilidad	35

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 D ha sido desarrollado para todos los proveedores de servicios que cumplan con los requisitos para realizar el Cuestionario de autoevaluación y para todos los comerciantes que no cumplan con las descripciones provistas en los cuestionarios A, B y C, descriptos brevemente en la siguiente tabla y explicados en detalle en *Instrucciones y directrices para completar el cuestionario de autoevaluación de las normas PCI DSS*.

Tipo de validación de SAQ	Descripción	SAQ
1	Comerciantes en cuyas transacciones la tarjeta no está presente (comercio electrónico, órdenes por teléfono o correo electrónico). Se terciarizan todas las funciones relativas a los datos de los titulares de tarjetas. <i>Esta clasificación no se aplica en ningún caso a comerciantes cuyas transacciones son personales.</i>	A
2	Comerciantes que solamente imprimen los datos de los titulares de tarjetas, pero no los almacenan electrónicamente.	B
3	Comerciantes con terminales independientes sin almacenamiento electrónico de los datos de los titulares de tarjetas.	B
4	Comerciantes con sistemas POS conectados a Internet. Sin almacenamiento electrónico de los datos de los titulares de tarjetas.	C
5	Todo comerciante (no incluido en las descripciones correspondientes a los cuestionarios SAQ A, B y C descriptos anteriormente) y todo proveedor de servicios que una marca de pago considere que cumpla con los requisitos para completar un Cuestionario de autoevaluación.	D

A fin de validar el cuestionario SAQ, los comerciantes que no cumplen con los criterios correspondientes a los cuestionarios SAQ A, B y C, descriptos anteriormente y todos los proveedores de servicios que una marca de pago considere que cumplan con los requisitos para completar un Cuestionario de evaluación, quedan definidos como Tipo 5, tanto en este documento como en las *Instrucciones y directrices para completar el cuestionario de autoevaluación de las normas PCI DSS*.

Si bien muchas de las organizaciones que completen cuestionarios SAQ D deberán validar el cumplimiento de todos los requisitos de las normas PCI DSS, es posible que algunos de estos requisitos no rijan para empresas con modelos comerciales muy específicos. Por ejemplo, una empresa que no utiliza tecnologías inalámbricas de ningún tipo, no deberá validar el cumplimiento de las secciones de las normas PCI DSS específicas para tecnologías inalámbricas. Consulte la guía que aparece a continuación para obtener información acerca de la exclusión de tecnologías inalámbricas y algunos otros requisitos específicos.

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 PCI DSS: pasos de conclusión

1. Complete el Cuestionario de autoevaluación (SAQ D) según las instrucciones incluidas en *Instrucciones y directrices para completar el cuestionario de autoevaluación de las normas PCI DSS*.
2. Realice un análisis de vulnerabilidad con un Proveedor Aprobado de Escaneo (ASV) del PCI SSC y solicítele al ASV pruebas de los análisis aprobados.
3. Complete la Declaración de cumplimiento en su totalidad.
4. Presente el SAQ, las pruebas del análisis aprobado y la Declaración de cumplimiento junto con todo otro documento solicitado al adquirente (en el caso de comerciantes), a la marca de pago o a todo otro solicitante (en el caso de proveedores de servicios).

Guía para la no aplicabilidad y exclusión de ciertos requisitos específicos

Exclusión: En caso de que deba responder el cuestionario SAQ D para validar el cumplimiento con las normas PCI DSS, es posible que se consideren las siguientes excepciones. Consulte “No aplicabilidad”, a continuación, para determinar la respuesta correcta.

- Las respuestas referidas a tecnologías inalámbricas deben responderse solo en caso de que cuente con dispositivos inalámbricos en alguna parte de la red (por ejemplo, Requisitos 1.2.3, 2.1.1 y 4.1.1). Tenga en cuenta que el Requisito 11.1 (utilización de un analizador inalámbrico) debe responderse aun si no cuenta con tecnologías inalámbricas en la red, ya que el analizador detecta todo dispositivo sin control o autorización que se haya añadido sin conocimiento del comerciante.
- Las preguntas relativas a las aplicaciones del cliente y los códigos (Requisito 6.3 a 6.5) deben responderse solo si su empresa desarrolla aplicaciones web propias.
- Las preguntas relativas a los Requisitos 9.1 a 9.4 deben responderse solo en el caso de que existan “áreas confidenciales”, según la definición del presente cuestionario. “Áreas confidenciales” hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan procesos o transmitan datos de los 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.

No aplicabilidad: Estos requisitos, y cualquier otro requisito que se considere 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 D: versión para el comerciante

Instrucciones para la presentación

El comerciante debe completar esta Declaración de cumplimiento para manifestar su estado de cumplimiento con 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 aplicables y consulte las instrucciones para presentar esta declaración en la sección “Cumplimiento de las PCI DSS: pasos de conclusión” de este documento.

Parte 1. Información de la empresa del Asesor de Seguridad Certificado (cuando corresponda)

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 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 adquiriente? Sí No

Parte 2c. Procesamiento de transacciones

Aplicación de pago en uso:

Versión de la aplicación de pago:

Parte 3. Validación de las PCI DSS

Según los resultados observados en el cuestionario SAQ D de fecha (*completion date*), (*Merchant Company Name*) declara que su 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 afirmativa, lo que da como resultado una clasificación general de **CUMPLIMIENTO**. Además, un Proveedor Aprobado de Escaneo del PCI SSC completó un análisis aprobado y, por tanto, (*Merchant Company Name*) ha demostrado cumplir con la totalidad de las PCI DSS.
- No conforme:** No se han completado todas las secciones del cuestionario SAQ de las normas PCI DSS o algunas respuestas obtuvieron "No" como respuesta, lo que da como resultado una clasificación general de **NO CONFORME**; o el Proveedor Aprobado de Escaneo del PCI SSC no ha completado un análisis aprobado y, por lo tanto, (*Merchant Company Name*) no ha sido capaz de demostrar el cumplimiento de la totalidad 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 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.*

Parte 3a. Confirmación del estado de cumplimiento

El comerciante confirma que:

- El Cuestionario de autoevaluación D de las normas PCI DSS, versión (*version of SAQ*), se completó según las instrucciones dadas.
- Toda la información que aparece dentro del cuestionario SAQ antes mencionado y en esta declaración muestran los resultados de la evaluación de manera equitativa en todos sus aspectos sustanciales.
- 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.
- He leído las normas PCI DSS y reconozco que debo cumplirlas en todo momento.
- No existe evidencia de almacenamiento de datos², de banda magnética (es decir, ninguna pista), datos de CAV2, CVC2, CID, o CVV2³, ni datos de PIN⁴ después de encontrarse la autorización de la transacción en TODOS los sistemas revisados durante la presente evaluación.

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 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> ↑	

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.*

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	
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 computadoras	<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"/>	
10	Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas	<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"/>	

Declaración de cumplimiento, SAQ D: versión para proveedor de servicios

Instrucciones para la presentación

El proveedor de servicios debe completar esta Declaración de cumplimiento para manifestar su estado de cumplimiento con 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 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 proveedor de servicios

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

Parte 2a. Servicios

Servicios prestados (marque todo lo que corresponda):

- | | | |
|---|--|---|
| <input type="checkbox"/> Autorización | <input type="checkbox"/> Programas de lealtad | <input type="checkbox"/> 3-D Secure Access Control Server |
| <input type="checkbox"/> Switching | <input type="checkbox"/> IPSP (Comercio electrónico) | <input type="checkbox"/> Transacciones con proceso de banda magnética |
| <input type="checkbox"/> Pasarela de pago | <input type="checkbox"/> Compensación y liquidación | <input type="checkbox"/> Proceso de transacciones por correo/teléfono |
| <input type="checkbox"/> Hosting | <input type="checkbox"/> Procesamiento de emisión | <input type="checkbox"/> 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 puertas de enlace y Web hosting, agentes de reservas aéreas, agentes de programas de lealtad, etc.)? Sí No

Parte 2c. Procesamiento de transacciones

¿De qué forma y en qué capacidad almacena, procesa y/o transmite su empresa los datos de titulares de tarjetas?

Aplicaciones de pago en uso o proporcionadas como parte del servicio:

Versión de la aplicación de pago:

Parte 3. Validación de las PCI DSS

Según los resultados observados en el cuestionario SAQ D de fecha (*completion date of SAQ*), (*Service Provider Company Name*) declara que su 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**. Además, un Proveedor Aprobado de Escaneo del PCI SSC completó un análisis aprobado y, por tanto, (*Service Provider Company Name*) ha demostrado cumplir con la totalidad de las PCI DSS.
- No conforme:** No se han completado todas las secciones del cuestionario SAQ del PCI o algunas respuestas obtuvieron "No" como respuesta, lo que da como resultado una clasificación general de **No conforme**; o el Proveedor Aprobado de Escaneo del PCI SSC no ha completado un análisis aprobado por lo tanto, (*Service Provider Company Name*) no ha sido capaz de demostrar el cumplimiento de la totalidad 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 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.*

Parte 3a. Confirmación del estado de cumplimiento

El proveedor de servicios confirma que:

- | | |
|--------------------------|---|
| <input type="checkbox"/> | El Cuestionario de autoevaluación D, versión (<i>insert version number</i>), se completó según 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"/> | He leído las normas PCI DSS y reconozco que debo cumplirlas en todo momento. |
| <input type="checkbox"/> | No existe evidencia de almacenamiento de datos ⁵ , de banda magnética (es decir, ninguna pista), datos de CAV2, CVC2, CID, o CVV2 ⁶ , ni datos de PIN ⁷ después de encontrarse la autorización de la transacción en TODOS los sistemas revisados durante la presente evaluación. |

Parte 3b. Confirmación del proveedor de servicios

<i>Firma del Oficial Ejecutivo del proveedor de servicios</i> ↑	<i>Fecha</i> ↑
<i>Nombre del Oficial Ejecutivo del proveedor de servicios</i> ↑	<i>Cargo</i> ↑

Nombre del proveedor de servicios representado ↑

⁵ 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.

⁶ 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).

⁷ 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	
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 computadoras	<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"/>	
10	Rastree y supervise los accesos a los recursos de red y a los datos de los titulares de las tarjetas	<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 D

Fecha de cumplimiento:

Desarrollar y mantener una red segura

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

Pregunta		Respuesta:	Sí	No	Especial*
1.1	¿Los estándares de configuración del firewall y el router incluyen lo siguiente?				
1.1.1	Un proceso formal para aprobar y evaluar todos los cambios y las conexiones de red externas en la configuración de los firewalls y los routers		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.2	Diagramas actualizados de la red con todas las conexiones que acceden a los datos de los titulares de las tarjetas, incluida toda red inalámbrica		<input type="checkbox"/>	<input type="checkbox"/>	
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		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.4	Descripción de grupos, de papeles y de responsabilidades para una administración lógica de los componentes de la red		<input type="checkbox"/>	<input type="checkbox"/>	
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		<input type="checkbox"/>	<input type="checkbox"/>	
1.1.6	Requisitos de revisión de las normas del firewall y del router, al menos, cada seis meses		<input type="checkbox"/>	<input type="checkbox"/>	
1.2	¿La configuración del firewall restringe las conexiones entre redes no confiables y cualquier tipo de sistema presente en el entorno del titular de la tarjeta del siguiente modo? <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>				
1.2.1.	Mediante restricciones del tránsito entrante y saliente a la cantidad que sea necesaria para el entorno de datos del titular de la tarjeta		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.2	Garantizando y sincronizando los archivos de configuración de routers		<input type="checkbox"/>	<input type="checkbox"/>	
1.2.3	Incluyendo instalaciones de firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configurando estos firewalls para negar y controlar (en caso de que ese tránsito fuera necesario para fines comerciales) todo tránsito desde el entorno inalámbrico hacia el entorno del titular de la tarjeta		<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:	Sí	No	Especial*
1.3	¿La configuración del firewall prohíbe el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas?				
1.3.1	¿Hay alguna zona DMZ implementada para limitar el tránsito entrante y saliente a los protocolos que sean necesarios en el entorno del titular de la tarjeta?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.2	¿Se encuentra el tránsito entrante de Internet restringido a las direcciones IP dentro de la DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.3	¿Las rutas directas están prohibidas para el tránsito de entrada o salida entre Internet y el entorno del titular de la tarjeta?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.4	¿Las direcciones internas tienen prohibido el paso desde Internet a la DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.5	¿Está restringido el tránsito saliente desde el entorno de datos del titular de la tarjeta hasta Internet de forma tal que el tránsito saliente sólo pueda acceder a direcciones IP dentro de la DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.6	¿Está implementada la inspección completa, o el filtro de paquete dinámico, para que solo las conexiones establecidas puedan entrar a la red?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.7	¿La base de datos está en una zona de red interna segregada de la DMZ?		<input type="checkbox"/>	<input type="checkbox"/>	
1.3.8	¿Se ha implementado la simulación IP con el fin de evitar que las direcciones internas se traduzcan y se divulguen en Internet mediante la utilización del espacio de dirección RFC 1918? <i>Utilice tecnologías de traducción de direcciones de red (NAT), por ejemplo traducción de direcciones de puertos (PAT).</i>		<input type="checkbox"/>	<input type="checkbox"/>	
1.4	¿Se ha instalado algún 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?		<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 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	¿Se cambian siempre los valores predeterminados de los proveedores antes de instalar un sistema en la red? <i>Algunos ejemplos son las contraseñas, las cadenas comunitarias de protocolo simple de administración de red (SNMP) y la eliminación de cuentas innecesarias.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
2.1.1	(a) Antes de instalar un sistema inalámbrico, ¿se han cambiado las opciones predeterminadas de los entornos inalámbricos conectados al entorno de datos del titular de la tarjeta o de los que transfieren datos del titular de la tarjeta? <i>**Algunos de los ejemplos de las opciones predeterminadas de los entornos inalámbricos son las claves de criptografía inalámbricas predeterminadas, las contraseñas y las cadenas comunitarias SNMP.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Está la configuración de seguridad de los dispositivos inalámbricos habilitada para la tecnología de cifrado de la autenticación y transmisión?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) ¿Se han desarrollado estándares de configuración para todos los componentes del sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Contemplan estos estándares todas las vulnerabilidades de seguridad conocidas y concuerdan con las normas de alta seguridad aceptadas en la industria, como SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST) y Center for Internet Security (CIS)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) ¿Garantizan los controles lo siguiente?				
2.2.1	La implementación de solamente una función principal por servidor		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.2	La desactivación de todos los servicios y protocolos innecesarios e inseguros, es decir, los servicios y protocolos que no sean directamente necesarios para desempeñar la función especificada de los dispositivos		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.3	¿Están configurados los parámetros de seguridad del sistema para evitar el uso indebido?		<input type="checkbox"/>	<input type="checkbox"/>	
2.2.4	¿Se han eliminado todas las funcionalidades innecesarias, como secuencias de comandos, controladores, funciones, subsistemas, sistemas de archivos y servidores web innecesarios?		<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>
2.3	<p>¿Está cifrado todo el acceso administrativo que no sea de consola?</p> <p><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></p>		<input type="checkbox"/>	<input type="checkbox"/>	
2.4	<p>Si es un proveedor de hosting compartido, ¿ha configurado los sistemas para proteger el entorno hosting y los datos de los titulares de tarjetas?</p> <p>Consulte el Anexo A: Requisitos adicionales de las PCI DSS para los proveedores de hosting compartido, para enterarse de los requisitos específicos que se deben cumplir.</p>		<input type="checkbox"/>	<input type="checkbox"/>	

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*
3.1	(a) ¿Se retienen los datos de los titulares de tarjetas lo mínimo necesario? ¿Se limita la cantidad de datos almacenados y el tiempo de retención al mínimo necesario para fines comerciales, legales o reglamentarios?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Existe alguna una política de retención y disposición de datos e incluye limitaciones como las descritas anteriormente en (a)?		<input type="checkbox"/>	<input type="checkbox"/>	
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	<p>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. NUNCA almacene el código de verificación de la tarjeta, el valor ni los elementos de datos del valor de verificación del PIN.</i></p> <p><i>Nota: Consulte el Glosario de términos, abreviaturas y acrónimos de las PCI DSS para obtener más información.</i></p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>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>		<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:	Sí	No	Especial*
3.3	<p>¿Se oculta el PAN cuando aparece (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerán)?</p> <p>Notas:</p> <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"/>	
3.4	<p>¿Se hace, como mínimo, ilegible el PAN en cualquier lugar donde se almacene (incluidos los datos almacenados en medios digitales portátiles, soporte de copias de respaldo y 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). Criptografía sólida con procesos y procedimientos de gestión de claves relacionadas. <p>La información de cuenta MÍNIMA que se debe dejar ilegible es el PAN.</p> <p>Si, por alguna razón, la empresa no puede hacer que el PAN sea ilegible, consulte el "Anexo B: Controles de compensación".</p> <p>Nota: La "criptografía sólida" se define en el Glosario de términos, abreviaturas y acrónimos de las PCI DSS.</p>		<input type="checkbox"/>	<input type="checkbox"/>	
3.4.1	Si se utiliza cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna):				
	(a) ¿El acceso lógico se administra 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)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Son las claves de descifrado independientes de las cuentas de usuario?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5	¿Están protegidas las claves criptográficas que se utilizan para cifrar los datos de los titulares de tarjetas contra la divulgación o el uso indebido?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.1	¿Está restringido el acceso a las claves criptográficas al número mínimo de custodios necesarios?		<input type="checkbox"/>	<input type="checkbox"/>	
3.5.2	¿Las claves criptográficas están protegidas de forma segura en la menor cantidad de ubicaciones posibles?		<input type="checkbox"/>	<input type="checkbox"/>	

Pregunta		Respuesta:	Sí	No	Especial*
3.6	(a) ¿Están completamente documentados e implementados todos los procesos y procedimientos de gestión de claves de las claves criptográficas que se usan para el cifrado de los datos de los titulares de tarjetas? (b) ¿Incluyen lo siguiente?		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.1	Generación de claves criptográficas sólidas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Distribución segura de claves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.3	Almacenamiento seguro de claves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.4	Cambio periódico 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 		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Destrucción o reemplazo de claves criptográficas antiguas o supuestamente en riesgo		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Divida el conocimiento y la creación del control dual de claves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	
3.6.7	Prevención de sustitución no autorizada de claves criptográficas		<input type="checkbox"/>	<input type="checkbox"/>	
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		<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:	Sí	No	Especial*
4.1	¿Se utiliza 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? <i>Algunos ejemplos de redes públicas abiertas que se encuentran dentro del ámbito de aplicación de las normas PCI DSS son Internet, las tecnologías inalámbricas, el sistema global de comunicaciones móviles (GSM) y el servicio de radio paquete general (GPRS).</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.

Pregunta		Respuesta:	<u>Sí</u>	<u>No</u>	<u>Especial*</u>
4.1.1	<p>¿Se utilizan las mejores prácticas de la industria (por ejemplo, IEEE 802.11i) en la implementación de cifrados sólidos para la autenticación y transmisión de redes inalámbricas que transfieren los datos de los titulares de tarjetas o están conectadas al entorno de datos de los titulares de tarjetas?</p> <p><i>Notas:</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>¿Hay políticas, procedimientos y prácticas establecidos para evitar que se envíen PANs no cifrados mediante tecnologías de mensajería de usuario final, como correo electrónico, mensajes instantáneos y chat?</p>		<input type="checkbox"/>	<input type="checkbox"/>	

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	¿Es implementado el software antivirus en todos los sistemas comúnmente afectados por software malicioso, en especial, computadoras personales y servidores?		<input type="checkbox"/>	<input type="checkbox"/>	
5.1.1	¿Son todos los programas antivirus capaces de detectar y eliminar todos los tipos conocidos de software malicioso y de proteger a los sistemas contra su ataque?		<input type="checkbox"/>	<input type="checkbox"/>	
5.2	¿Todos los mecanismos antivirus son actuales y capaces de generar registros de auditoría? ¿Están en funcionamiento?		<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 instalados por los proveedores?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Los parches críticos de seguridad se instalan después 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"/>	
6.2	(a) ¿Existe algún proceso establecido para identificar las vulnerabilidades de seguridad recientemente descubiertas (por ejemplo, la subscripción a los servicios de alerta disponibles de forma gratuita mediante de Internet)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Los estándares de configuración se actualizan conforme al Requisito 2.2 de las normas PCI DSS para subsanar cualquier otro problema de vulnerabilidad?		<input type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) ¿Existen aplicaciones de software desarrolladas de acuerdo a las normas PCI DSS (por ejemplo, inicio de sesión y autenticación seguras) sobre la base de las mejores prácticas de la industria e incorporan la seguridad de la información durante el ciclo de desarrollo de software?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Garantizan los controles lo siguiente?				

* “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:	Sí	No	Especial*
6.3.1	Las pruebas de todos los parches de seguridad y la configuración del sistema y del software cambian antes de su despliegue, incluidas, entre otras, las siguientes pruebas:		<input type="checkbox"/>	<input type="checkbox"/>	
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.)		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.2	Validación de un correcto manejo de los errores		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.3	Validación del almacenamiento criptográfico seguro		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.4	Validación de las comunicaciones seguras		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.1.5	Validación de un correcto control del acceso basado en funciones (RBAC)		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.2	Desarrollo/prueba por separado y entornos de producción		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.3	Separación de funciones entre desarrollo/prueba y entornos de producción		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.4	Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo		<input type="checkbox"/>	<input type="checkbox"/>	
6.3.5	Eliminación de datos y cuentas de prueba antes de que se activen los sistemas de producción		<input type="checkbox"/>	<input type="checkbox"/>	
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		<input type="checkbox"/>	<input type="checkbox"/>	
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 <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 exige el Requisito 6.3 de las normas PCI DSS. 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>		<input type="checkbox"/>	<input type="checkbox"/>	
6.4	(a) ¿Se siguen los procedimientos de control de todos los cambios en los componentes del sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Garantizan los procedimientos lo siguiente?				
6.4.1	Documentación de incidencia		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Aprobación de la gerencia a cargo de las partes pertinentes		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.3	Pruebas de la funcionalidad operativa		<input type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Procedimientos de desinstalación		<input type="checkbox"/>	<input type="checkbox"/>	

Pregunta		Respuesta:	Sí	No	Especial*
6.5	(a) ¿Se han desarrollado todas las aplicaciones web (internas y externas, que incluyan acceso administrativo web a la aplicación) según las directrices de codificación segura, como la <i>Guía para proyectos de seguridad de aplicaciones web abierta</i> ?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Está cubierta la prevención de las vulnerabilidades de codificación comunes en los procesos de desarrollo de software, incluidas las siguientes? <i>Nota: En la guía OWASP, las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el punto 6.5.10 eran actuales al momento de publicación de las normas PCI DSS v1.2. Sin embargo, cuando se actualice la guía OWSAP (llegado el caso), debe utilizarse la versión actual sobre estos requisitos.</i>				
6.5.1	Lenguaje de comandos entre distintos sitios (XSS)		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Errores de inyección, en especial, errores de inyección SQL <i>También considere los errores de inyección LDAP y Xpath, así como otros errores de inyección.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Ejecución de archivos maliciosos		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.4	Referencias inseguras a objetos directos		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Falsificación de solicitudes entre distintos sitios (CSRF)		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.6	Filtración de información y manejo inadecuado de errores		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.7	Autenticación y administración de sesión interrumpidas		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.8	Almacenamiento criptográfico inseguro		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Comunicaciones inseguras		<input type="checkbox"/>	<input type="checkbox"/>	
6.5.10	Omisión de restringir el acceso URL		<input type="checkbox"/>	<input type="checkbox"/>	
6.6	En cuanto a las aplicaciones web públicas ¿se tratan las nuevas amenazas y vulnerabilidades de continuo, y se las protege contra ataques conocidos aplicando <i>alguno</i> de los siguientes métodos? <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 capa de aplicación web enfrente de aplicaciones web públicas. 		<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 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"/>	
	(b) ¿Incluyen las limitaciones de acceso lo siguiente?				
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		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.2	La asignación de privilegios se basa en la tarea del personal individual, su clasificación y función		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.3	Los requisitos de un formulario de autorización escrito por la gerencia que detalle los privilegios solicitados		<input type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Implementación de un sistema de control de acceso automático		<input type="checkbox"/>	<input type="checkbox"/>	
7.2	(a) ¿Existe un sistema de control de acceso para los sistemas con varios usuarios que restrinja el acceso según la necesidad del usuario de obtener información y que esté configurado para "negar todos" a menos que se lo permita específicamente?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) Este sistema de control de acceso debe incluir lo siguiente:				
7.2.1	Cobertura de todos los componentes del sistema		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.2	La asignación de privilegios a individuos se basa en la clasificación del trabajo y la función		<input type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Ajuste predeterminado "negar todos"		<input type="checkbox"/>	<input type="checkbox"/>	

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

Pregunta		Respuesta:	Sí	No	Especial*
8.1	¿Se designa a cada usuario con una ID única antes de ser autorizado a acceder a componentes del sistema y a datos de los titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
8.2	Además de la asignación de una ID única, ¿se utiliza uno o más de los siguientes métodos para autenticar a todos los usuarios? <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) 		<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:	Sí	No	Especial*
8.3	¿Se encuentra incorporada 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? <i>Utilice tecnologías tales como autenticación remota y servicio dial-in (RADIUS); o sistemas de control de acceso mediante control del acceso desde terminales (TACACS) con tokens; o VPN (basada en SSL/TLS o IPSEC) con certificados individuales.</i>		<input type="checkbox"/>	<input type="checkbox"/>	
8.4	¿Se vuelven todas las contraseñas ilegibles durante la transmisión y almacenamiento de todos los componente de sistema que utilizan tecnologías de criptografía sólida (definida en el <i>Glosario de términos, abreviaturas y acrónimos de las normas DSS PCI y PA-DDS</i>)?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5	¿Se han implementado los controles adecuados para 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?				
8.5.1	¿Se controlan el agregado, la eliminación y la modificación de las ID de usuario, las credenciales y otros objetos de identificación?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.2	¿Se verifica la identidad del usuario antes de restablecer contraseñas?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.3	¿Se configuran la primera contraseña en un valor único para cada usuario, la cual deberá cambiarse de inmediato después del primer uso?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.4	¿Se cancela de inmediato el acceso para cualquier usuario cesante?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.5	¿Se eliminan o desactivan las cuentas de usuario inactivas al menos cada 90 días?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.6	¿Se activan las cuentas utilizadas por proveedores para el mantenimiento remoto únicamente durante el período necesario?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.7	¿Se hacen saber los procedimientos y las políticas de contraseñas a todos los usuarios que tengan acceso a datos de titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.8	¿Se prohíben las cuentas y contraseñas grupales, compartidas o genéricas?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.9	¿Debe cambiarse la contraseña de usuario al menos cada 90 días?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.10	¿Se requiere una contraseña de al menos siete caracteres de extensión?		<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:	Sí	No	Especial*
8.5.11	¿Se utilizan contraseñas que contengan tanto caracteres numéricos como alfabéticos?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.12	¿Es necesario que una persona envíe una contraseña nueva diferente de cualquiera de las últimas cuatro contraseñas que utilizó?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.13	¿Están limitados los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.14	¿Se encuentra la duración del bloqueo configurada en un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.15	Si alguna sesión estuvo inactiva durante más de 15 minutos, ¿debe el usuario reescribir la contraseña para que se active nuevamente la terminal?		<input type="checkbox"/>	<input type="checkbox"/>	
8.5.16	¿Están autenticados 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.)		<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*
9.1	¿Existen controles de entrada a la empresa para limitar y supervisar el acceso a sistemas en el entorno de datos de titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.1	(a) ¿Hay cámaras de video u otros mecanismos de control de acceso para supervisar el acceso físico de personas a áreas confidenciales? <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>		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Se revisan y relacionan a otras entradas los datos obtenidos de las cámaras de video?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) ¿Se conservan los datos obtenidos de cámara de video por un período no menor a tres meses a menos que la ley estipule lo contrario?		<input type="checkbox"/>	<input type="checkbox"/>	
9.1.2	¿Se encuentra restringido el acceso físico a conexiones de red de acceso público?		<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:	Sí	No	Especial*
9.1.3	¿Se encuentra restringido el acceso físico a puntos de acceso inalámbrico, puertas de enlace y dispositivos manuales?		<input type="checkbox"/>	<input type="checkbox"/>	
9.2	<p>¿Existen 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.</i></p> <p><i>"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>		<input type="checkbox"/>	<input type="checkbox"/>	
9.3	¿Se trata a todos los visitantes de la siguiente manera?				
9.3.1	¿Se los autoriza previamente al ingreso a áreas en las que se procesan o se conservan datos de titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.2	¿Se le otorga un token físico (por ejemplo una placa de identificación o dispositivo de acceso) con vencimiento que identifique a los visitantes como personas no pertenecientes a la empresa?		<input type="checkbox"/>	<input type="checkbox"/>	
9.3.3	¿Se les solicita entregar del token físico antes de salir de las instalaciones de la empresa o al momento del vencimiento?		<input type="checkbox"/>	<input type="checkbox"/>	
9.4	(a) ¿Se utiliza un registro de visitas para implementar una pista de auditoría física de la actividad de visitas?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Figuran en el registro el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico?		<input type="checkbox"/>	<input type="checkbox"/>	
	(c) ¿Se conserva el registro de visitas durante tres meses como mínimo, a menos que la ley estipule lo contrario?		<input type="checkbox"/>	<input type="checkbox"/>	
9.5	(a) ¿Se almacenan 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?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Se revisa la seguridad del lugar al menos una vez al año?		<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"/>	
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"/>	
	(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"/>	
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"/>	

Pregunta		Respuesta:	Sí	No	Especial*
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"/>	
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"/>	
9.9.1	(a) ¿Se mantienen adecuadamente los registros de inventario de todos los medios?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Se realizan inventarios de medios, al menos, una vez al año?		<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"/>	
9.10.1	¿Se pasan los materiales impresos por una trituradora, se incineran o reducen a pulpa de modo que sea imposible reconstruirlos?		<input type="checkbox"/>	<input type="checkbox"/>	
9.10.2	¿Se destruyen los medios electrónicos con los datos de titulares de tarjetas para que dichos datos no puedan reconstruirse?		<input type="checkbox"/>	<input type="checkbox"/>	

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:	Respuesta:		
			Sí	No	Especial*
10.1	¿Existe algún proceso para vincular todos los accesos a componentes del sistema (especialmente el acceso con privilegios administrativos, tales como los de raíz) a cada usuario en particular?		<input type="checkbox"/>	<input type="checkbox"/>	
10.2	¿Hay pistas de auditoría automatizadas implementadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos?				
10.2.1	Todo acceso de personas a datos de titulares de tarjetas		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.2	Todas las acciones realizadas por personas con privilegios de raíz o administrativos		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.3	Acceso a todas las pistas de auditoría		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.4	Intentos de acceso lógico no válidos		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.5	Uso de mecanismos de identificación y autenticación		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.6	Inicialización de los registros de auditoría		<input type="checkbox"/>	<input type="checkbox"/>	
10.2.7	Creación y eliminación de objetos en el nivel del sistema		<input type="checkbox"/>	<input type="checkbox"/>	
10.3	¿Se encuentran registradas las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento?				
10.3.1	Identificación de usuarios		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.2	Tipo de evento		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.3	Fecha y hora		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.4	Indicación de éxito u omisión		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.5	Origen del evento		<input type="checkbox"/>	<input type="checkbox"/>	
10.3.6	Identidad o nombre de los datos, componentes del sistema o recurso afectados		<input type="checkbox"/>	<input type="checkbox"/>	
10.4	¿Están sincronizados todos los relojes y horarios críticos del sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5	(a) ¿Están resguardadas todas las pistas de auditoría para evitar que se alteren?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Garantizan los controles lo siguiente?				
10.5.1	¿Está limitada la visualización de pistas de auditoría a quienes lo necesiten por motivos de trabajo?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.2	¿Se encuentran todos los archivos de pistas protegidos de alteraciones sin autorización?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.3	¿Se realiza una copia de seguridad rápida de las pistas de auditoría en un servidor de registros central o medios que resulten difíciles de modificar?		<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	Sí	No	Especial*
10.5.4	¿Se escriben los registros para tecnologías externas en un servidor de registros en la LAN interna?		<input type="checkbox"/>	<input type="checkbox"/>	
10.5.5	¿Se utiliza el software de monitorización de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta)?		<input type="checkbox"/>	<input type="checkbox"/>	
10.6	<p>¿Se revisan los registros de todos los componentes del sistema al menos una vez al día</p> <p><i>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).</i></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>		<input type="checkbox"/>	<input type="checkbox"/>	
10.7	¿Se conserva el historial de pista de auditorías, con un mínimo de tres meses de duración, durante al menos un año, para su análisis inmediato (por ejemplo, en línea, archivado o recuperable para la realización de copias de seguridad)?		<input type="checkbox"/>	<input type="checkbox"/>	

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	<p>¿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)?</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>		<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	Sí	No	Especial*
11.3	(a) ¿Se realizan pruebas de penetración externas e internas al menos una vez al año y después de cualquier actualización o modificación importante 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)?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Incluyen estas pruebas de penetración los siguientes elementos?				
11.3.1	¿Pruebas de penetración de capa de red?		<input type="checkbox"/>	<input type="checkbox"/>	
11.3.2	¿Pruebas de penetración de capa de aplicación?		<input type="checkbox"/>	<input type="checkbox"/>	
11.4	(a) ¿Se utilizan sistemas de detección y/o prevención de intrusiones para supervisar el tráfico en el entorno de datos de titulares de tarjetas y alertar al personal ante la sospecha de riesgos?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Se mantienen actualizados todos los motores de detección y prevención de intrusiones?		<input type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) ¿Se ha implementado el software para la supervisión de integridad de archivos con el fin de alertar al personal ante modificaciones no autorizadas de archivos críticos del sistema, archivos de configuración o archivos de contenido?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Se ha configurado el software para realizar comparaciones de archivos críticos al menos semanalmente? <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>		<input type="checkbox"/>	<input type="checkbox"/>	

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"/>	
12.1.1 ¿Aborda todos los requisitos de las normas PCI DSS?		<input type="checkbox"/>	<input type="checkbox"/>	
12.1.2 ¿Incluye un proceso anual para identificar las amenazas, las vulnerabilidades y los resultados en una evaluación formal de riesgos?		<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"/>	
12.2 ¿Se desarrollan 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)?		<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"/>	
(b) ¿Requieren estas políticas de uso lo siguiente?				
12.3.1 Aprobación explícita de la gerencia		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.2 Autenticación para el uso de la tecnología		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.3 Una lista de todos los dispositivos y personal que tenga acceso		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.4 Etiquetado de dispositivos con propietario, información de contacto y objetivo		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.5 Usos aceptables de la tecnología		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.6 Ubicaciones aceptables de las tecnologías en la red		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.7 Lista de productos aprobados por la empresa		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.8 Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad		<input type="checkbox"/>	<input type="checkbox"/>	
12.3.9 Activación de tecnologías de acceso remoto para proveedores sólo cuando estos lo requieren, con desactivación automática después de la utilización		<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	Sí	No	Especial*
12.3.10	Las organizaciones que utilicen esta sección deben completar la Hoja de trabajo para controles de compensación o la Hoja de trabajo para explicaciones de no aplicabilidad, según corresponda. Ambos formularios se encuentran en el Anexo.		<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?				
12.5.1	¿El establecimiento, la documentación y la distribución de políticas y procedimientos de seguridad?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.2	¿La supervisión y el análisis de alertas de seguridad y la distribución de información al personal correspondiente?		<input type="checkbox"/>	<input type="checkbox"/>	
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"/>	
12.5.4	¿La administración de las cuentas de usuario, incluidas las adiciones, eliminaciones y modificaciones?		<input type="checkbox"/>	<input type="checkbox"/>	
12.5.5	¿La supervisión y el control de todos los datos de acceso?		<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"/>	
12.6.1	¿Se capacita a los empleados al contratarlos al menos una vez al año?		<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2	¿Se le exige 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?		<input type="checkbox"/>	<input type="checkbox"/>	
12.7	¿Se examina a los posibles empleados (consulte la definición de “empleado” 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>		<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"/>	

* “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	Sí	No	Especial*
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"/>	
12.9	¿Se ha implementado un plan de respuesta a incidentes que incluirá los siguientes elementos para responder de inmediato a un fallo en el sistema?				
12.9.1	(a) ¿Se ha implementado un plan de respuesta a incidentes en caso de que ocurra una falla en el sistema?		<input type="checkbox"/>	<input type="checkbox"/>	
	(b) ¿Aborda este plan al menos lo siguiente?				
	▪ Funciones, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago.		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Procedimientos específicos de respuesta a incidentes.		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Procedimientos de recuperación y continuidad comercial.		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ procesos de realización de copia de seguridad de datos;		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Análisis de los requisitos legales para el informe de riesgos.		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Cobertura y respuestas de todos los componentes críticos del sistema.		<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago.		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.2	¿Se prueba el plan al menos una vez al año?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.3	¿Se ha designado personal especializado disponible las 24 horas de día, los siete días de la semana para responder a las alertas?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.4	¿Se proporciona una capacitación adecuada al personal responsable de la respuesta ante fallos de seguridad?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.5	¿Se incluyen alertas de sistemas de detección y prevención de intrusiones, y de monitorización de integridad de archivos?		<input type="checkbox"/>	<input type="checkbox"/>	
12.9.6	¿Se ha elaborado e implementado un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria?		<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: Requisitos de las PCI DSS adicionales para proveedores de hosting compartido

Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de los titulares de tarjetas

Pregunta		Respuesta	Sí	No	Especial*
A.1	<p>¿Se encuentran los datos y entornos sujetos al hosting de las entidades protegidos (es decir comerciante, proveedor de servicio u otra entidad), según A.1.1 a A.1.4?</p> <p><i>Un proveedor de hosting debe cumplir con estos requisitos, así como también con las demás secciones correspondientes de PCI DSS.</i></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>				
A.1.1	¿Realiza cada entidad procesos con acceso al entorno de datos de titulares de tarjetas de la entidad?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.2	¿Se encuentran los privilegios y accesos de cada entidad restringidos a su propio entorno de datos de titulares de tarjetas?		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.3	<p>¿Están habilitados los registros y las pistas de auditoría?</p> <p>¿Son exclusivos para el entorno de datos de titulares de tarjetas de cada entidad y cumplen con el Requisito 10 de las normas PCI DSS?</p>		<input type="checkbox"/>	<input type="checkbox"/>	
A.1.4	¿Está habilitados los procesos para proporcionar una investigación forense oportuna en caso de riesgos para un comerciante o proveedor de servicios alojado?		<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 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>

