



**Norma de seguridad de datos  
de la Industria de tarjetas de pago (PCI)  
Cuestionario de autoevaluación A  
y Atestación de cumplimiento**

---

**Comerciantes con tarjetas ausentes,  
todas las funciones que impliquen el manejo de  
datos del titular de la tarjeta totalmente tercerizadas  
Para su uso con la Versión 3.2.1 de la PCI DSS**

Junio de 2018

## Modificaciones realizadas a los documentos

Fecha	Versión de las PCI DSS	Revisión del SAQ	Descripción
Octubre de 2008	1.2		Alinear el contenido con la nueva versión 1.2 de PCI DSS e implementar cambios menores notados desde la versión 1.1 original.
Octubre de 2010	2.0		Para alinear el contenido con los requisitos y procedimientos de prueba de PCI DSS v2.0
Febrero de 2014	3.0		Para alinear el contenido con los requisitos y procedimientos de prueba de PCI DSS v3.0 e incorporar opciones de respuesta adicionales.
Abril de 2015	3.1		Se actualizó para conseguir alineación con las PCI DSS v3.1. Para conocer en detalle los cambios de las PCI DSS, consulte <i>PCI DSS – Resumen de cambios de las PCI DSS versión 3.0 a 3.1</i> .
Julio de 2015	3.1	1.1	Se actualizó la numeración de la versión para conseguir alineación con otros SAQ.
Abril de 2016	3.2	1.0	Se actualizó para conseguir alineación con las PCI DSS v3.2. Para conocer en detalle los cambios de las PCI DSS, consulte <i>PCI DSS – Resumen de cambios de las PCI DSS versión 3.1 a 3.2</i> . Requisitos añadidos de PCI DSS v3.2 Requisitos 2, 8 y 12.
Enero de 2017	3.2	1.1	Cambios de documento actualizados para aclarar los requisitos añadidos en la actualización de abril de 2016. Se agregó nota a pie de página a la sección Antes de comenzar para aclarar la intención de la inclusión de los Requisitos 2 y 8 de PCI DSS.
Junio de 2018	3.2.1	1.0	Se actualizó para conseguir alineación con las PCI DSS v3.2.1. Para conocer en detalle los cambios de las PCI DSS, consulte <i>PCI DSS – Resumen de cambios de las PCI DSS versión 3.2 a 3.2.1</i> . Requisito añadido 6.2 de PCI DSS v3.2.1.

### DECLARACIONES:

*La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerarse, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.*

# Índice

<b>Modificaciones realizadas a los documentos .....</b>	<b>i</b>
<b>Antes de comenzar .....</b>	<b>iii</b>
<b>Pasos para la realización de la autoevaluación de las PCI DSS .....</b>	<b>iv</b>
<b>Comprensión del cuestionario de autoevaluación .....</b>	<b>iv</b>
<i>Pruebas esperadas.....</i>	<i>iv</i>
<b>Respuestas del cuestionario de autoevaluación .....</b>	<b>v</b>
<b>Guía para la no aplicabilidad de ciertos requisitos específicos.....</b>	<b>v</b>
<b>Excepción legal</b>	<b>v</b>
<b>Sección 1: Información sobre la evaluación .....</b>	<b>1</b>
<b>Sección 2: Cuestionario de autoevaluación A .....</b>	<b>4</b>
<b>Desarrolle y mantenga redes y sistemas seguros.....</b>	<b>4</b>
<i>Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.....</i>	<i>4</i>
<b>Mantener un programa de administración de vulnerabilidad.....</b>	<b>5</b>
<i>Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros.....</i>	<i>5</i>
<b>Implementar medidas sólidas de control de acceso .....</b>	<b>6</b>
<i>Requisito 8: Identifique y autentique el acceso a los componentes del sistema. ....</i>	<i>6</i>
<i>Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta .....</i>	<i>7</i>
<b>Mantener una política de seguridad de información .....</b>	<b>9</b>
<i>Requisito 12: Mantener una política que aborde la seguridad de la información para todo el personal .....</i>	<i>9</i>
<b>Anexo A: Requisitos adicionales de las PCI DSS.....</b>	<b>11</b>
<i>Anexo A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido.....</i>	<i>11</i>
<i>Anexo A2: Requisitos de PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana para conexiones de terminal de POS POI de la tarjeta presente.....</i>	<i>11</i>
<i>Anexo A3: Validación suplementaria de las entidades designadas (DES).....</i>	<i>11</i>
<b>Anexo B: Hoja de trabajo de controles de compensación .....</b>	<b>12</b>
<b>Anexo C: Explicaciones de no aplicabilidad.....</b>	<b>13</b>
<b>Sección 3: Detalles de la validación y la atestación .....</b>	<b>14</b>

## Antes de comenzar

---

El SAQ A se ha desarrollado para contemplar los requisitos aplicables a los comerciantes cuyas funciones que impliquen el manejo de datos del titular de la tarjeta están totalmente tercerizadas a terceros validados, y cuando los comerciantes solamente conservan informes en papel o recibos con los datos del titular de la tarjeta.

Los comerciantes correspondientes al SAQ A pueden ser comerciantes de comercio electrónico, pedido por correo o pedido por teléfono (comerciantes con tarjetas ausentes) y no almacenan, procesan ni transmiten datos de titulares de tarjeta en formato electrónico en sus sistemas o instalaciones.

Los comerciantes correspondientes al SAQ A confirman que para este canal de pago:

- Su empresa maneja solamente transacciones con tarjeta ausente (comercio electrónico y órdenes por correo/teléfono);
- Todo el procesamiento de los datos de los titulares de las tarjetas se terceriza en su totalidad a procesadores de pagos externos validados por las PCI DSS;
- Su empresa no almacena, procesa ni transmite en forma electrónica datos de los titulares de tarjetas en sus sistemas o locales, sino que depende completamente de un uno o varios terceros que realizan estas funciones;
- Su empresa ha confirmado que todos los terceros que manejan el almacenamiento, el procesamiento o la transmisión de los datos del titular de la tarjeta cumplen con las PCI DSS.
- Su empresa retiene solamente informes o recibos en papel con datos del titular de la tarjeta, y estos documentos no se reciben por medios electrónicos.

Además, para los canales de comercio electrónico:

- La totalidad de todas las páginas de pago que se entregan al explorador del consumidor tienen su origen directamente en los proveedores de servicios externos validados por las PCI DSS.

### ***Este SAQ no se aplica a los canales cara a cara.***

Esta versión abreviada del SAQ incluye preguntas que se aplican a un tipo específico de entorno de pequeños comerciantes, tal como se define en los criterios de elegibilidad. Si hay requisitos de las PCI DSS aplicables a su entorno que no están cubiertos en este SAQ, puede ser una indicación de que este SAQ no es adecuado para su entorno. Además, de cualquier modo debe cumplir con todos los requisitos de PCI DSS para cumplir con las PCI DSS.

**Nota:** Para este SAQ, los requisitos PCI DSS que abordan la protección de sistemas informáticos (por ejemplo, Requisitos 2, 6 y 8) se aplican a los comerciantes de comercio electrónico que redirigen a los clientes desde su sitio web a un tercero para el procesamiento de pagos, y específicamente al servidor web del comerciante en el que se encuentra el mecanismo de redirección. Los comerciantes de pedido por teléfono/correo (MOTO) o los de comercio electrónico que han tercerizado completamente todas las operaciones (donde no hay un mecanismo de redirección desde el comerciante al tercero) y por lo tanto no tienen ningún sistema en el alcance de este SAQ, considerarían estos requisitos como “no aplicables”. Consulte la guía en las siguientes páginas para saber cómo informar los requisitos que no son aplicables.

## Pasos para la realización de la autoevaluación de las PCI DSS

1. Además, identifica el SAQ para su entorno.—Consulte el documento *Instrucciones y pautas del SAQ* en el sitio web del PCI SSC para obtener más información.
2. Confirmar que su entorno cuenta con la delimitación del alcance apropiada y que cumple los criterios de elegibilidad para el SAQ que está usando (según se define en la Parte 2g de la Atestación de cumplimiento).
3. Evalúe su entorno respecto del cumplimiento con los requisitos aplicables de las PCI DSS.
4. Complete todas las secciones que correspondan de este documento:
  - Sección 1 (Partes 1 y 2 de la AOC): Información de la evaluación y Resumen ejecutivo
  - Sección 2: Cuestionario de Autoevaluación de las PCI DSS (SAQ A)
  - Sección 3 (Partes 3 y 4 de la AOC): Detalles de la validación y la atestación y Plan de acción para los requisitos de no cumplimiento (si corresponden)
5. Presente el SAQ y la Atestación de cumplimiento (AOC), junto con cualquier otro documento solicitado, como los informes de análisis de ASV al adquiriente, a la marca de pago o a otro solicitante.

## Comprensión del cuestionario de autoevaluación

Las preguntas que se encuentran en la columna “Pregunta de las PCI DSS” de este cuestionario de autoevaluación están realizadas en función de los requisitos presentes en las PCI DSS.

Asimismo, se han proporcionado recursos adicionales que brindan pautas respecto de los requisitos de las PCI DSS y sobre la forma en que debe completarse el cuestionario de autoevaluación para asistir con el proceso de evaluación. A continuación se proporciona una descripción general de algunos de estos recursos que se mencionaron:

Documento	Incluye:
PCI DSS <i>(Requisitos de la norma de seguridad de datos de la PCI y procedimientos de evaluación de seguridad)</i>	<ul style="list-style-type: none"> <li>• Pautas para la delimitación del alcance</li> <li>• Pautas referidas al propósito que subyace todos los requisitos de las PCI DSS</li> <li>• Detalles de los procedimientos de prueba</li> <li>• Pautas sobre los controles de compensación</li> </ul>
Documentos con instrucciones y pautas de SAQ	<ul style="list-style-type: none"> <li>• Información respecto de todos los SAQ y los criterios de elegibilidad que presentan</li> <li>• Método para determinar qué SAQ es el apropiado para su organización</li> </ul>
<i>Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS</i>	<ul style="list-style-type: none"> <li>• Descripciones y definiciones de los términos utilizados en las PCI DSS y los cuestionarios de autoevaluación</li> </ul>

Tanto estos como otros recursos útiles se encuentran en el sitio web del PCI SSC ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)). Se recomienda a las organizaciones que analicen las PCI DSS y otra documentación de respaldo existente antes de comenzar una evaluación.

### Pruebas esperadas

Las instrucciones que se presentan en la columna “Pruebas esperadas” se corresponden con los procedimientos de prueba indicados en las PCI DSS, y ofrecen una descripción con detalles de los tipos de actividades implicados en las pruebas que deben realizarse a los fines de verificar el cumplimiento con un requisito. En las PCI DSS se ofrecen detalles completos sobre los procedimientos de prueba para cada requisito.

## Respuestas del cuestionario de autoevaluación

Para cada pregunta, existe una selección de respuestas para dar cuenta del estado de la empresa en relación con ese requisito. **Se puede seleccionar únicamente una respuesta para cada pregunta.**

En la tabla a continuación se proporciona una descripción del significado para cada respuesta:

Respuesta	Cuándo utilizar esta respuesta:
Sí	La prueba esperada se ha realizado, y todos los elementos del requisito se han cumplido tal como se estipulaba.
Sí con CCW (Hoja de trabajo de controles de compensación)	<p>La prueba esperada se ha realizado, y todos los requisitos se han cumplido con ayuda de un control de compensación.</p> <p>Todas las respuestas en esta columna requieren que se complete una Hoja de trabajo de controles de compensación (CCW) en el Anexo B del SAQ.</p> <p>La información respecto del uso de los controles de compensación y las pautas para completar la hoja de trabajo se proporcionan en las PCI DSS.</p>
No	Algunos de los elementos presentes en el requisito, o todos ellos, no se han cumplido, están en proceso de implementarse o es necesario realizar más pruebas antes de poder establecer si están implementados.
N/C (No corresponde)	<p>El requisito no se aplica al entorno de la organización. (Consulte la Guía para la no aplicabilidad de ciertos requisitos específicos que se ofrece debajo para conocer ejemplos).</p> <p>Todas las respuestas en esta columna requieren una explicación de respaldo en el Anexo C del SAQ.</p>

## Guía para la no aplicabilidad de ciertos requisitos específicos

Si alguno de los requisitos se considera como no aplicable en el caso de su entorno, seleccione la opción "N/C" para ese requisito en particular y complete la hoja de trabajo "Explicaciones de no aplicabilidad" en el Anexo C para cada entrada "N/C".

## Excepción legal

Si su organización está sujeta a una restricción legal que impide que cumpla con un requisito de las PCI DSS, marque la columna "No" correspondiente a dicho requisito y complete la atestación relevante en la Parte 3.

## Sección 1: Información sobre la evaluación

### Instrucciones para la presentación

Este documento debe completarse como una declaración de los resultados que tuvo la autoevaluación del comerciante con los *Requisitos de la Norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) y procedimientos de evaluación de seguridad*. Complete todas las secciones que correspondan: El comerciante es responsable de asegurarse que las partes relevantes completen cada sección según corresponda: Comuníquese con el adquiriente (banco comercial) o las marcas de pago para establecer los procedimientos para la presentación y elaboración del informe.

### Parte 1. Información sobre Comerciante y Asesor de Seguridad Certificado

#### Parte 1a. Información de la organización del comerciante

Nombre de la empresa:		DBA (operando bajo el nombre de):	
Nombre del contacto:		Cargo:	
Teléfono:		Correo electrónico:	
Dirección comercial:		Ciudad:	
Estado/Provincia:		País:	
			Código postal:
URL:			

#### Parte 1b. Información de la empresa del evaluador de seguridad certificado (QSA) (si corresponde)

Nombre de la empresa:			
Nombre del contacto del QSA principal:		Cargo:	
Teléfono:		Correo electrónico:	
Dirección comercial:		Ciudad:	
Estado/Provincia:		País:	
			Código postal:
URL:			

### Parte 2. Resumen ejecutivo

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

Comercio minorista     
  Telecomunicaciones     
  Tiendas de comestibles y supermercado  
 Petróleo     
  Comercio electrónico     
  Pedidos por correo/teléfono (MOTO)  
 Otros (especifique):

¿Cuáles son los tipos de canales de pago a los que presta servicios su empresa?

- Pedidos por correo/teléfono (MOTO)  
 Comercio electrónico  
 Tarjeta presente (en persona)

¿Cuáles son los canales de pago que este SAQ abarca?

- Pedidos por correo/teléfono (MOTO)  
 Comercio electrónico  
 Tarjeta presente (en persona)

**Nota:** Si su organización cuenta con un canal de pago o un proceso que este SAQ no abarca, comuníquese con su adquiriente o marca de pago respecto de la validación para los otros canales.

## Parte 2. Resumen ejecutivo (continuación)

### Parte 2b. Descripción del negocio de tarjeta de pago

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

### Parte 2c. Ubicaciones

Indique los tipos de instalaciones y un resumen de las ubicaciones que se encuentran incluidas en la revisión de las PCI DSS (por ejemplo, tiendas minoristas, oficinas corporativas, centros de datos, centros de llamadas, etc.).

Tipo de instalación	Número de instalaciones de este tipo	Ubicaciones de las instalaciones (ciudad, país)
<i>Ejemplo: Tiendas minoristas</i>	3	<i>Boston, MA, EE. UU.</i>

### Parte 2d. Aplicación de pago

¿La organización utiliza una aplicación de pago o más de una?  Sí  No

Proporcione la siguiente información relativa a las aplicaciones de pago que su organización utiliza:

Nombre de la aplicación de pago	Número de versión:	Proveedor de la aplicación	¿Se encuentra la aplicación en la lista de las PA-DSS?	Fecha de vencimiento de la lista de las PA-DSS (si corresponde)
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	
			<input type="checkbox"/> Sí <input type="checkbox"/> No	

### Parte 2e. Descripción del entorno

Proporcione una descripción **general** del entorno que esta evaluación abarca.

*Por ejemplo:*

- *Conexiones hacia y desde el entorno de datos del titular de la tarjeta (CDE).*
- *Componentes importantes que hay dentro del entorno de datos del titular de la tarjeta, incluidos los dispositivos POS, las bases de datos, los servidores web, etc. y cualquier otro componente de pago necesario, según corresponda.*

¿Su empresa utiliza la segmentación de red para influir en el alcance del entorno de las PCI DSS?

Sí  No

*(Consulte la sección "Segmentación de red" de las PCI DSS para obtener información acerca de la segmentación de red).*



## Parte 2. Resumen ejecutivo (continuación)

### Parte 2f. Proveedores de servicio externos

¿Su empresa utiliza un Integrador o revendedor certificado (QIR)?  Sí  No

#### En caso de ser Sí:

Nombre de la empresa QIR:

Nombre individual del QIR:

Descripción de los servicios proporcionados por QIR:

¿Su empresa comparte los datos de los titulares de tarjeta con uno o más proveedores de servicio externos (por ejemplo, Integrador o revendedor certificado (QIR), empresas de puertas de enlace, procesadores de pago, proveedores de servicio de pago (PSP), empresas de Web hosting, agentes de reservas en aerolíneas, agentes del programa de lealtad, etc.)?  Sí  No

#### En caso de ser Sí:

Nombre del proveedor de servicios:

Descripción de los servicios proporcionados:

Nombre del proveedor de servicios:	Descripción de los servicios proporcionados:

**Nota:** El requisito 12.8 rige para todas las entidades en esta lista.

### Parte 2g. Elegibilidad para completar el SAQ A

El comerciante certifica que es elegible para completar esta versión abreviada del Cuestionario de autoevaluación porque, para este canal de pago:

- El comerciante maneja solamente transacciones con tarjeta ausente (comercio electrónico y órdenes por correo/teléfono);
- Todo el procesamiento de los datos de los titulares de las tarjetas se terceriza en su totalidad a procesadores de pagos externos validados por las PCI DSS;
- El comerciante no almacena, procesa ni transmite en forma electrónica datos de los titulares de tarjetas en sus sistemas o locales, sino que depende completamente de uno o varios terceros que realizan estas funciones;
- El comerciante ha confirmado que el tercero o los terceros que manejan el almacenamiento, el procesamiento y/o la transmisión de los datos de los titulares de tarjetas cumplen con las PCI DSS; **y**
- El comerciante retiene solamente informes o recibos en papel con datos de los titulares de tarjetas, y estos documentos no se reciben por medios electrónicos.
- Además, para los canales de comercio electrónico:  
La totalidad de todas las páginas de pago que se entregan al explorador del consumidor tienen su origen directamente en los proveedores de servicios externos validados por las PCI DSS.

## Sección 2: Cuestionario de autoevaluación A

**Nota:** Las siguientes preguntas están numeradas de acuerdo con los requisitos y procedimientos de prueba de las PCI DSS, tal como se definen en el documento de los Procedimientos de evaluación de seguridad y requisitos de las PCI DSS.

Fecha de realización de la autoevaluación:

### Desarrolle y mantenga redes y sistemas seguros

**Requisito 2:** *No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad*

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
2.1 (a) ¿Se cambian siempre los valores predeterminados por el proveedor antes de instalar un sistema en la red?  <i>Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS (puntos de venta), las aplicaciones de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.</i>	<ul style="list-style-type: none"> <li>▪ Revisar las políticas y los procedimientos.</li> <li>▪ Examinar la documentación del proveedor.</li> <li>▪ Observar las configuraciones del sistema y las configuraciones de cuenta.</li> <li>▪ Entrevistar al personal.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se eliminan o desactivan las cuentas predeterminadas que no son necesarias antes de instalar un sistema en la red?	<ul style="list-style-type: none"> <li>▪ Revisar las políticas y los procedimientos.</li> <li>▪ Revisar la documentación del proveedor.</li> <li>▪ Examinar las configuraciones del sistema y las configuraciones de cuenta.</li> <li>▪ Entrevistar al personal.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Mantener un programa de administración de vulnerabilidad

### Requisito 6: *Desarrollar y mantener sistemas y aplicaciones seguros*

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta <i>(Marque únicamente una respuesta para cada pregunta)</i>			
			Sí	Sí con CCW	No	N/C
6.2	(a) ¿Están todos los programas de software y componentes del sistema protegidos de las vulnerabilidades conocidas mediante parches de seguridad instalados proporcionados por los proveedores?	<ul style="list-style-type: none"> <li>Revisar las políticas y los procedimientos.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se instalan parches de seguridad crítica en un lapso de un mes contado a partir de su fecha de lanzamiento?	<ul style="list-style-type: none"> <li>Revisar las políticas y los procedimientos.</li> <li>Examinar los componentes del sistema.</li> <li>Comparar la lista de los parches de seguridad instalados con las listas de parches de proveedor recientes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Implementar medidas sólidas de control de acceso

**Requisito 8: Identifique y autentique el acceso a los componentes del sistema.**

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
8.1.1	¿Se asigna a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema o a los datos de titulares de tarjetas?	<ul style="list-style-type: none"> <li>Revisar los procedimientos de contraseña.</li> <li>Entrevistar al personal.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	¿Se desactiva o elimina de manera inmediata el acceso de cualquier usuario cesante?	<ul style="list-style-type: none"> <li>Revisar los procedimientos de contraseña.</li> <li>Examinar las cuentas de usuarios cesantes.</li> <li>Revisar las listas de acceso actuales.</li> <li>Observar los dispositivos de autenticación física devueltos.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2	<p>¿Además de asignar una ID única, se emplean uno o más de los siguientes métodos para autenticar a todos los usuarios?</p> <ul style="list-style-type: none"> <li>Algo que el usuario sepa, como una contraseña o frase de seguridad</li> <li>Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente</li> <li>Algo que el usuario sea, como un rasgo biométrico</li> </ul>	<ul style="list-style-type: none"> <li>Revisar los procedimientos de contraseña.</li> <li>Observar los procesos de autenticación.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.3	<p>(a) ¿Los parámetros de la contraseña del usuario se encuentran configurados de manera que exijan que las contraseñas/frases de contraseña cumplan con los siguientes requisitos?</p> <ul style="list-style-type: none"> <li>Longitud de contraseña mínima de siete caracteres</li> <li>Combinación de caracteres numéricos y alfabéticos</li> </ul> <p>De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.</p>	<ul style="list-style-type: none"> <li>Examinar los parámetros de configuración del sistema para verificar los parámetros de la contraseña.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
8.5 ¿Se prohíben las cuentas y contraseñas grupales, compartidas o genéricas u otros métodos de autenticación, de la siguiente manera? <ul style="list-style-type: none"> <li>▪ Las ID de usuario y cuentas genéricas se inhabilitan o eliminan;</li> <li>▪ No existen las ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas; y</li> <li>▪ ¿No se utilizan las identificaciones de usuario compartidas y genéricas para administrar componentes del sistema?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Revisar las políticas y los procedimientos.</li> <li>▪ Examinar las listas de identificaciones de usuario.</li> <li>▪ Entrevistar al personal.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
9.5 ¿Todos los medios de almacenamiento están físicamente asegurados (incluyendo, sin sentido limitativo, computadoras, medios extraíbles electrónicos, recibos en papel, informes de papel y faxes)?  <i>A los efectos del Requisito 9, "medios" se refiere a todos los medios en papel y electrónicos que contienen datos de titulares de tarjetas.</i>	<ul style="list-style-type: none"> <li>▪ Revisar las políticas y los procedimientos para el resguardo seguro de los medios.</li> <li>▪ Entrevistar al personal.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6 (a) ¿Se lleva un control estricto sobre la distribución interna o externa de cualquier tipo de medios de almacenamiento?	<ul style="list-style-type: none"> <li>▪ Revisar las políticas y los procedimientos para la distribución de los medios.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Incluyen los controles lo siguiente:					

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
9.6.1	¿Están clasificados los medios de manera que se pueda determinar la confidencialidad de los datos?	<ul style="list-style-type: none"> <li>Revisar las políticas y los procedimientos para la clasificación de los medios.</li> <li>Entrevistar al personal de seguridad.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	¿Los medios se envían por correo seguro u otro método de envío que se pueda rastrear con precisión?	<ul style="list-style-type: none"> <li>Entrevistar al personal.</li> <li>Examinar los registros de seguimiento de la distribución de medios y los documentos relacionados.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	¿Se obtiene la aprobación de la administración antes de que se trasladen los medios (especialmente cuando se distribuyen a personas)?	<ul style="list-style-type: none"> <li>Entrevistar al personal.</li> <li>Examinar los registros de seguimiento de la distribución de medios y los documentos relacionados.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	¿Se lleva un control estricto sobre el almacenamiento y accesibilidad de los medios?	<ul style="list-style-type: none"> <li>Revisar las políticas y los procedimientos.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	(a) ¿Se destruyen los medios cuando ya no sean necesarios para la empresa o por motivos legales?	<ul style="list-style-type: none"> <li>Revisar las políticas y los procedimientos para la destrucción periódica de medios.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Se realiza la destrucción de la siguiente manera?:					
9.8.1	(a) ¿Se cortan en tiras, incineran o hacen pasta los materiales de copias en papel para que no se puedan reconstruir los datos de titulares de tarjetas?	<ul style="list-style-type: none"> <li>Revisar las políticas y los procedimientos para la destrucción periódica de medios.</li> <li>Entrevistar al personal.</li> <li>Observar los procesos.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se destruirán de forma segura los contenedores que almacenan los materiales con información para impedir acceso al contenido?	<ul style="list-style-type: none"> <li>Examinar la seguridad de los contenedores de almacenamiento.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Mantener una política de seguridad de información

### Requisito 12: Mantener una política que aborde la seguridad de la información para todo el personal

**Nota:** A los fines del Requisito 12, "personal" se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que "residan" en las instalaciones de la entidad o que tengan acceso al entorno de datos de los titulares de tarjetas en la empresa.

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
12.8	¿Se mantienen e implementan políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta de la siguiente manera?				
12.8.1	¿Se mantiene una lista de los proveedores de servicios, incluida una descripción de los servicios prestados?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	¿Se mantiene un acuerdo por escrito que incluye el reconocimiento de que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente?  <b>Nota:</b> La redacción exacta del reconocimiento dependerá del acuerdo existente entre las dos partes, los detalles del servicio prestado y las responsabilidades asignadas a cada parte. No es necesario que el reconocimiento incluya el texto exacto de este requisito.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	¿Existe un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
12.8.4	¿Se mantiene un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor de servicios con una frecuencia anual, como mínimo?	<ul style="list-style-type: none"> <li>Observar los procesos.</li> <li>Revisar las políticas y los procedimientos, así como la documentación complementaria.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	¿Se conserva la información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad?	<ul style="list-style-type: none"> <li>Observar los procesos.</li> <li>Revisar las políticas y los procedimientos, así como la documentación complementaria.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.1	(a) ¿Se ha creado un plan de respuesta a incidentes para implementarlo en caso de fallos en el sistema?	<ul style="list-style-type: none"> <li>Revisar el plan de respuesta a incidentes.</li> <li>Revisar los procesos del plan de respuesta a incidentes.</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## **Anexo A: Requisitos adicionales de las PCI DSS**

### ***Anexo A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido***

Este anexo no se utiliza durante las evaluaciones de comerciantes.

### ***Anexo A2: Requisitos de PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana para conexiones de terminal de POS POI de la tarjeta presente***

Este anexo no se utiliza durante las evaluaciones de comerciantes de los SAQ A.

### ***Anexo A3: Validación suplementaria de las entidades designadas (DESV)***

Este Anexo se aplica únicamente a las entidades designadas por una marca de pago o adquirente que exige una validación adicional de los requisitos de la PCI DSS existentes. Las entidades que necesitan validar este Anexo deberán utilizar la Plantilla suplementaria de presentación de informes y la Atestación de cumplimiento suplementaria para presentación de informes de DESV, y consultar con la marca de pago y/o adquirente del caso los procedimientos de presentación.

## Anexo B: 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 con CCW”.

**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.

Consulte los anexos B, C y D de las PCI DSS para obtener información respecto del uso de los controles de compensación y las pautas para completar la hoja de trabajo.

### Definición y número de requisito:

	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.	



## Sección 3: Detalles de la validación y la atestación

### Parte 3. Validación de la PCI DSS

Esta AOC se basa en los resultados observados en el SAQ A (Sección 2), con fecha (*fecha de finalización del SAQ*).

Según los resultados observados en el SAQ A mencionado anteriormente, los firmantes que se identifican en las Partes 3b-3d, según corresponda, hacen valer el siguiente estado de cumplimiento de la entidad identificada en la Parte 2 del presente documento: (*marque una*):

<input type="checkbox"/>	<p><b>En cumplimiento:</b> Se han completado todas las secciones del SAQ de la PCI DSS y se ha respondido afirmativamente a todas las preguntas, lo que resulta en una calificación general de <b>EN CUMPLIMIENTO</b>, y (<i>nombre de la empresa del comerciante</i>) ha demostrado un cumplimiento total con la PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Falta de cumplimiento:</b> No se han completado todas las secciones del SAQ de la PCI DSS o se ha respondido en forma negativa a algunas de las preguntas, lo que resulta en una calificación general de <b>FALTA DE CUMPLIMIENTO</b>, y (<i>nombre de la empresa del comerciante</i>) no ha demostrado un cumplimiento total con la PCI DSS.</p> <p><b>Fecha objetivo</b> para el cumplimiento:</p> <p>Es posible que se exija a una entidad que presente este formulario con un estado de Falta de cumplimiento que complete el Plan de acción en la Parte 4 de este documento. <i>Consulte con su adquirente o la(s) marca(s) de pago antes de completar la Parte 4.</i></p>						
<input type="checkbox"/>	<p><b>En cumplimiento pero con una excepción legal:</b> Uno o más requisitos están marcados como “No” debido a una restricción legal que impide el cumplimiento con un requisito. Esta opción requiere una revisión adicional del adquirente o la marca de pago.</p> <p><i>Si está marcado, complete lo siguiente:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Requisito afectado</th> <th>Detalles respecto de cómo la limitación legal impide que se cumpla el requisito</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Requisito afectado	Detalles respecto de cómo la limitación legal impide que se cumpla el requisito				
Requisito afectado	Detalles respecto de cómo la limitación legal impide que se cumpla el requisito						

### Parte 3a. Reconocimiento de estado

Los firmantes confirman:

(*marque todo lo que corresponda*)

<input type="checkbox"/>	El cuestionario de autoevaluación A de las PCI DSS, Versión ( <i>número de la versión del SAQ</i> ), se completó de acuerdo con las instrucciones correspondientes.
<input type="checkbox"/>	Toda la información dentro del arriba citado SAQ y en esta atestación representa razonablemente los resultados de mi evaluación en todos los aspectos sustanciales.
<input type="checkbox"/>	He confirmado con mi proveedor de la aplicación de pago que mi sistema de pago no almacena datos confidenciales de autenticación después de la autorización.
<input type="checkbox"/>	He leído la PCI DSS y reconozco que debo mantener el pleno cumplimiento de dicha norma, según se aplica a mi entorno, en todo momento.
<input type="checkbox"/>	Si ocurre un cambio en mi entorno, reconozco que debo evaluar nuevamente mi entorno e implementar los requisitos adicionales de las PCI DSS que correspondan.

### Parte 3. Validación de la PCI DSS (continuación)

#### Parte 3a. Reconocimiento de estado(cont.)

<input type="checkbox"/>	No existe evidencia de almacenamiento de datos completos de la pista <sup>1</sup> , datos de CAV2, CVC2, CID, o CVV2 <sup>2</sup> , ni datos de PIN <sup>3</sup> después de encontrarse la autorización de la transacción en NINGÚN sistema revisado durante la presente evaluación.
<input type="checkbox"/>	Los análisis del ASV completados por un Proveedor aprobado de escaneo (ASV) certificado por el PCI SSC ( <i>nombre del ASV</i> )

#### Parte 3b. Declaración del comerciante

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

#### Parte 3c. Reconocimiento del Evaluador de seguridad certificado (QSA) (si corresponde)

Si un QSA participó o brindó ayuda durante esta evaluación, describa la función realizada:	
--	--

<i>Firma del Oficial debidamente autorizado de la empresa del QSA</i> ↑	<i>Fecha:</i>
<i>Nombre del Oficial debidamente autorizado:</i>	<i>Empresa de QSA:</i>

#### Parte 3d. Participación del Asesor de seguridad interna (ISA) (si corresponde)

Si un ISA participó o brindó ayuda durante esta evaluación, describa al Personal de ISA y describa la función realizada:	
--	--

<sup>1</sup> Datos codificados en la banda magnética, o su equivalente, utilizada para la autorización durante una transacción con tarjeta presente. Es posible que las entidades no retengan los datos completos de la pista después de la autorización de la transacción. Los únicos elementos de los datos de la pista que se pueden retener son el número de cuenta principal (PAN), la fecha de vencimiento y el nombre del titular de la tarjeta.

<sup>2</sup> El valor de tres o cuatro dígitos impreso junto al panel de firma, o en el frente de una tarjeta de pago, que se utiliza para verificar las transacciones sin tarjeta presente.

<sup>3</sup> El número de identificación personal ingresado por el titular de la tarjeta durante una transacción con tarjeta presente o el bloqueo de PIN cifrado presente en el mensaje de la transacción.

## Parte 4. Plan de acción para los requisitos por falta de cumplimiento

Seleccione la respuesta apropiada para “En cumplimiento con los requisitos de las PCI DSS” correspondiente para cada requisito. Si la respuesta a cualquier requisito es “No”, debe proporcionar la fecha en la que la empresa espera cumplir 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.

Requisito de las PCI DSS*	Descripción del requisito	En cumplimiento con los requisitos de las PCI DSS (seleccione uno)		Fecha y medidas de corrección (si se seleccionó “NO” para algún requisito)
		SÍ	NO	
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"/>	
6	Desarrolle y mantenga sistemas y aplicaciones seguros.	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identificar y autenticar el acceso a los componentes del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrinja el acceso físico a datos de titulares de tarjetas.	<input type="checkbox"/>	<input type="checkbox"/>	
12	Mantenga una política que aborde la seguridad de la información para todo el personal.	<input type="checkbox"/>	<input type="checkbox"/>	

\* Los requisitos de las PCI DSS indicados aquí se refieren a las preguntas en la Sección 2 del SAQ.

