Norma de seguridad de datos de la Industria de tarjetas de pago (PCI)

Cuestionario de autoevaluación B y Atestación de cumplimiento

Comerciantes con validadoras manuales o terminales independientes con discado externo solamente. Sin almacenamiento electrónico de los datos de los titulares de tarjetas

Para su uso con la Versión 3.2 de las PCI DSS

Revisión 1.1

Enero de 2017

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 *PCI DSS – Resumen de cambios de las PCI DSS versión 3.0 a 3.1*.
Julio de 2015	3.1	1.1	Se actualizó para eliminar las referencias a las "mejores prácticas" antes del 30 de junio de 2015.
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 *PCI DSS – Resumen de cambios de las PCI DSS versión 3.1 a 3.2.*
Enero de 2017	3.2	1.1	Se actualizó la numeración de la versión para conseguir alineación con otros SAQ

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

Antes de comenzar

El SAQ B se ha desarrollado para contemplar los requisitos aplicables a los comerciantes que procesan datos de los titulares de tarjetas solamente por medio de validadoras manuales o terminales independientes con discado externo. Los comerciantes que se corresponden al SAQ B pueden ser comerciantes con instalaciones físicas (con la tarjeta presente) o pedido por correo/teléfono (tarjeta no presente), y que no almacenan datos de titulares de tarjetas en ningún sistema informático.

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

- Su empresa usa solamente máquinas impresoras y/o terminales independientes con discado externo (conectados a través la línea telefónica a su procesador) para registrar la información de la tarjeta de pago de sus clientes;
- Los terminales independientes con discado externo no están conectados a ningún otro sistema en su entorno;
- Los terminales independientes con discado externo no están conectados a Internet;
- Su empresa no transmite datos de los titulares de tarjetas por la red (ni a través de una red interna ni de Internet.
- Su empresa retiene solamente reportes o recibos en papel con datos de los titulares de tarjetas, y estos documentos no se reciben por medios electrónicos; **y**
- Su empresa no almacena datos del titular de la tarjeta en formato electrónico.

Este SAQ no es aplicable a los canales de comercio electrónico.

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.

Pasos para la realización de la autoevaluación de las PCI DSS

1. Identificar el SAQ para su entorno; consulte el documento *Instrucciones y directrices del SAQ* en el sitio web del PCI SSC para obtener 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 B)
    - 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 *(Requisitos de la norma de seguridad de datos de la PCI y procedimientos de evaluación de seguridad)*	• Pautas para la delimitación del alcance • Pautas referidas al propósito que subyace todos los requisitos de las PCI DSS • Detalles de los procedimientos de prueba • Pautas sobre los controles de compensación
Documentos con instrucciones y pautas de SAQ	• Información respecto de todos los SAQ y los criterios de elegibilidad que presentan • Método para determinar qué SAQ es el apropiado para su organización
Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS	• Descripciones y definiciones de los términos utilizados en las PCI DSS y los cuestionarios de autoevaluación

Tanto estos como otros recursos útiles se encuentran en el sitio web del PCI SSC *(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)	La prueba esperada se ha realizado, y todos los requisitos se han cumplido con ayuda de un control de compensación. 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. 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.
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)	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). Todas las respuestas en esta columna requieren una explicación de respaldo en el Anexo C del SAQ.

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, selecciones 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 supermercados
☐ 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?	¿Cuáles son los canales de pago que este SAQ abarca?
☐ Pedidos por correo/teléfono (MOTO)	☐ Pedidos por correo/teléfono (MOTO)
☐ Comercio electrónico	☐ Comercio electrónico
☐ Tarjeta presente (en persona)	☐ 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 adquirente o marca de pago respecto de la validación para los otros canales.*

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)
Ejemplo: Tiendas minoristas	*3*	*Boston, MA, EE. UU.*

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)
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ No	
			☐ Sí ☐ 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? *(Consulte la sección "Segmentación de red" de las DSS PCI para obtener información acerca de la segmentación de red).*	☐ Sí ☐ No

Parte 2f. Proveedores de servicio externos

¿Su empresa utiliza un Integrador o revendedor certificado (QIR)? En caso de ser Sí: Nombre de la empresa QIR: Nombre individual del QIR: Descripción de los servicios proporcionados por QIR:	☐ Sí ☐ No
¿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:**

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

Parte 2g. Elegibilidad para completar el SAQ B

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

☐	El comerciante utiliza solamente validadoras manuales para imprimir la información relativa a la tarjeta de pago del cliente y no transfiere datos de los titulares de tarjetas por teléfono o Internet; o

	El comerciante utiliza terminales independientes con discado externo (conectados mediante una línea telefónica a su procesador), que no están conectadas a Internet ni a ningún otro sistema dentro del entorno del comerciante.
☐	El comerciante no transmite datos de los titulares de tarjetas por la red (ni a través de una red interna ni de Internet);
☐	El comerciante no almacena datos del titular de la tarjeta en formato electrónico; **y**
☐	Si el comerciante almacena datos del titular de la tarjeta, éstos solo están en informes impresos o copias de recibos impresos y no se reciben electrónicamente.

Sección 2: Cuestionario de autoevaluación B

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:

Proteger los datos del titular de la tarjeta

Requisito 3: Proteger los datos almacenados 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
3.2	(c) ¿Se eliminan o se convierten en irrecuperables los datos de autenticación confidenciales al finalizar el proceso de autorización?	▪ Revisar las políticas y los procedimientos ▪ Examinar las configuraciones del sistema ▪ Examinar los procesos de eliminación	☐	☐	☐	☐
	(d) ¿Todos los sistemas se adhieren a los siguientes requisitos de no almacenamiento de datos de autenticación confidenciales después de la autorización (incluso si son cifrados)?					

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
3.2.1	¿No se almacena el contenido completo de pista de la banda magnética (ubicada en el reverso de la tarjeta, datos equivalentes que están 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.* ***Nota:*** *En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:* • *El nombre del titular de la tarjeta.* • *Número de cuenta principal (PAN).* • *Fecha de vencimiento.* • *Código de servicio* *Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.*	▪ Examinar fuentes de datos, incluidas las siguientes: • Datos de transacciones entrantes • Todos los registros • Archivos de historial • Archivos de seguimiento • Esquemas de bases de datos • Contenidos de bases de datos	☐	☐	☐	☐
3.2.2	¿Después de la autorización se almacena el código o valor de verificación de la tarjeta (número de tres o cuatro dígitos impresos en el anverso o el reverso de una tarjeta de pago)?	▪ Examinar fuentes de datos, incluidas las siguientes: • Datos de transacciones entrantes • Todos los registros • Archivos de historial • Archivos de seguimiento • Esquemas de bases de datos • Contenidos de bases de datos	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
3.2.3	¿No se almacena el número de identificación personal (PIN) ni el bloqueo del PIN cifrado después de la autorización?	▪ Examinar fuentes de datos, incluidas las siguientes: • Datos de transacciones entrantes • Todos los registros • Archivos de historial • Archivos de seguimiento • Esquemas de bases de datos • Contenidos de bases de datos	☐	☐	☐	☐
3.3	¿Está oculto el PAN cuando aparece (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda verlo completo como se indica a continuación? ***Nota:*** *Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, requisitos legales o de las marcas de las tarjetas de pago para los recibos de POS [puntos de venta]).*	▪ Revisar las políticas y los procedimientos ▪ Revisar las funciones que necesitan acceso a las vistas del PAN completo ▪ Examinar las configuraciones del sistema ▪ Observar las vistas del PAN	☐	☐	☐	☐

Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
4.2	(b) ¿Se han puesto en práctica políticas que especifiquen que no se deben enviar números PAN sin protección a través de las tecnologías de mensajería del usuario final?	▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐

Implementar medidas sólidas de control de acceso

Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	**Sí con CCW**	**No**	**N/C**
7.1	¿Se limita el acceso a los componentes del sistema y a los datos de titulares de tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso, de la manera siguiente?:					
7.1.2	¿El acceso a las identificaciones de usuario con privilegios está restringido según se indica a continuación? ▪ ¿Restringidos a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo? ▪ ¿Asignado solamente a las funciones que específicamente necesitan acceso privilegiado?	▪ Examinar la política de control de acceso escrita ▪ Entrevistar al personal ▪ Entrevistar a la administración ▪ Revisar las identificaciones de los usuarios con privilegios	☐	☐	☐	☐
7.1.3	¿El acceso se asigna según la tarea, la clasificación y la función de cada persona?	▪ Examinar la política de control de acceso escrita ▪ Entrevistar a la administración ▪ Revisar las identificaciones de los usuarios	☐	☐	☐	☐

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)? *A los efectos del Requisito 9, "medios" se refiere a todos los medios en papel y electrónicos que contienen datos de titulares de tarjetas.*	▪ Revisar las políticas y los procedimientos para el resguardo seguro de los medios ▪ Entrevistar al personal	☐	☐	☐	☐
9.6	(a) ¿Se lleva un control estricto sobre la distribución interna o externa de cualquier tipo de medios de almacenamiento?	▪ Revisar las políticas y los procedimientos para la distribución de los medios	☐	☐	☐	☐
	(b) ¿Incluyen los controles lo siguiente:					
9.6.1	¿Están clasificados los medios de manera que se pueda determinar la confidencialidad de los datos?	▪ Revisar las políticas y los procedimientos para la clasificación de los medios ▪ Entrevistar al personal de seguridad	☐	☐	☐	☐
9.6.2	¿Los medios se envían por correo seguro u otro método de envío que se pueda rastrear con precisión?	▪ Entrevistar al personal ▪ Examinar los registros de seguimiento de la distribución de medios y los documentos relacionados	☐	☐	☐	☐
9.6.3	¿Se obtiene la aprobación de la administración antes de que se trasladen los medios (especialmente cuando se distribuyen a personas)?	▪ Entrevistar al personal ▪ Examinar los registros de seguimiento de la distribución de medios y los documentos relacionados	☐	☐	☐	☐
9.7	¿Se lleva un control estricto sobre el almacenamiento y accesibilidad de los medios?	▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
9.8	(a) ¿Se destruyen los medios cuando ya no sean necesarios para la empresa o por motivos legales?	▪ Revisar las políticas y los procedimientos para la destrucción periódica de medios	☐	☐	☐	☐
	(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?	• Revisar las políticas y los procedimientos para la destrucción periódica de medios • Entrevistar al personal • Observar los procesos	☐	☐	☐	☐
	(b) ¿Se destruirán de forma segura los contenedores que almacenan los materiales con información para impedir acceso al contenido?	• Revisar las políticas y los procedimientos para la destrucción periódica de medios • Examinar la seguridad de los contenedores de almacenamiento	☐	☐	☐	☐
9.9	¿Están protegidos los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta contra alteraciones y sustituciones? ***Nota:*** *Este requisito rige para los dispositivos de lectura de tarjetas que se usan en transacciones (es decir, al pasar o deslizar la tarjeta) en los puntos de venta. Este requisito no pretende regir los componentes de ingreso manual de claves, como teclados de computadoras y teclados numéricos de POS.*					
	(a) ¿Las políticas y los procedimientos requieren que se mantenga una lista de dichos dispositivos?	▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐
	(b) ¿Las políticas y los procedimientos requieren que los dispositivos se inspeccionen periódicamente para buscar intentos de alteración o sustitución?	▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐
	(c) ¿Las políticas y los procedimientos requieren que el personal esté capacitado para que detecten comportamientos sospechosos e informen la alteración o sustitución de dispositivos?	▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
9.9.1	(a) ¿En la lista de dispositivos se incluye lo siguiente? • Marca y modelo del dispositivo • Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) • Número de serie del dispositivo u otro método de identificación única	▪ Examinar la lista de dispositivos	☐	☐	☐	☐
	(b) ¿La lista es precisa y está actualizada?	▪ Observar los dispositivos y las ubicaciones de los dispositivos y comparar con la lista	☐	☐	☐	☐
	(c) ¿Se actualiza la lista cuando se agregan, reubican y desactivan los dispositivos?	▪ Entrevistar al personal	☐	☐	☐	☐
9.9.2	(a) ¿Se inspeccionan periódicamente las superficies de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento)? ***Nota:*** *Entre los ejemplos de indicios de que un dispositivo puede haber sido alterado o sustituido, se pueden mencionar accesorios inesperados o cables conectados al dispositivo, etiquetas de seguridad faltantes o cambiadas, carcasas rotas o con un color diferente o cambios en el número de serie u otras marcas externas.*	▪ Entrevistar al personal ▪ Observar los procesos de inspección y comparar con los procesos definidos	☐	☐	☐	☐
	(b) ¿El personal conoce los procedimientos para inspeccionar los dispositivos?	▪ Entrevistar al personal	☐	☐	☐	☐
9.9.3	¿Está capacitado el personal para que detecten indicios de alteración o sustitución en los dispositivos?					

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
	(a) ¿El material de capacitación para el personal que trabaja en los puntos de venta incluye lo siguiente? • Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de autorizarlos a acceder y modificar un dispositivo o solucionar algún problema. • No instalar, cambiar ni devolver dispositivos sin verificación. • Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). • Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).	▪ Revisar los materiales de capacitación	☐	☐	☐	☐
	(b) ¿El personal que trabaja en los puntos de venta recibió capacitación, y conoce los procedimientos que se emplean en la detección y realización de informes en casos de indicios de alteración o sustitución de los dispositivos?	▪ Entrevistar al personal en los puntos de venta	☐	☐	☐	☐

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
12.1	¿Existe una política de seguridad establecida, publicada, mantenida y divulgada al todo el personal pertinente?	▪ Revisar la política de seguridad de información	☐	☐	☐	☐
12.1.1	¿Se revisa la política de seguridad, al menos, una vez al año y se la actualiza cuando se realizan cambios en el entorno?	▪ Revisar la política de seguridad de información ▪ Entrevistar al personal a cargo	☐	☐	☐	☐
12.3	¿Hay desarrolladas políticas de uso para las tecnologías críticas que definen cómo usarlas correctamente y que exijan lo siguiente? ***Nota:*** *Ejemplos de tecnologías críticas incluyen, entre otros, las tecnologías inalámbricas y de acceso remoto, las computadoras portátiles, las tabletas, los medios electrónicos extraíbles, el uso del correo electrónico y el uso de Internet.*					
12.3.1	¿Aprobación explícita de las partes autorizadas para utilizar las tecnologías?	▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo	☐	☐	☐	☐
12.3.3	¿Una lista de todos los dispositivos y el personal que tenga acceso?	▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo	☐	☐	☐	☐
12.3.5	¿Usos aceptables de la tecnología?	▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo	☐	☐	☐	☐
12.4	¿Las políticas y los procedimientos de seguridad definen claramente las responsabilidades de seguridad de la información de todo el personal?	▪ Revisar las políticas y los procedimientos de seguridad de información ▪ Entrevistar a una muestra del personal a cargo	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
12.5	(b) ¿Las siguientes responsabilidades de administración de seguridad de la información están asignadas a una persona o equipo?					
12.5.3	¿Establecimiento, documentación y distribución de los procedimientos de respuesta ante incidentes de seguridad y escalación para garantizar un manejo oportuno y efectivo de todas las situaciones?	▪ Revisar las políticas y los procedimientos de seguridad de información	☐	☐	☐	☐
12.6	(a) ¿Se ha implementado un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de los procedimientos y de la política de seguridad de los datos del titular de la tarjeta?	▪ Revisar el programa de concienciación sobre seguridad	☐	☐	☐	☐
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?	▪ Revisar las políticas y los procedimientos ▪ Observar los procesos ▪ Revisar la lista de proveedores de servicios.	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
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? ***Nota:*** *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.*	▪ Observar los acuerdos escritos ▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐
12.8.3	¿Existe un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso?	▪ Observar los procesos ▪ Revisar las políticas y los procedimientos así como la documentación complementaria	☐	☐	☐	☐
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?	▪ Observar los procesos ▪ Revisar las políticas y los procedimientos así como la documentación complementaria	☐	☐	☐	☐
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?	▪ Observar los procesos ▪ Revisar las políticas y los procedimientos así como la documentación complementaria	☐	☐	☐	☐
12.10.1	(a) ¿Se ha creado un plan de respuesta a incidentes para implementarlo en caso de fallos en el sistema?	▪ Revisar el plan de respuesta a incidentes ▪ Revisar los procesos del plan de respuesta a incidentes	☐	☐	☐	☐

Anexo A: Requisitos adicionales de la 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 la PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana

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

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.	

Anexo C: Explicaciones de no aplicabilidad

Si la columna "N/C" (No corresponde) se marcó en el cuestionario, utilice esta hoja de trabajo para explicar por qué el requisito relacionado no se aplica a su organización.

Requisito	Razón por la cual el requisito no es aplicable
Ejemplo:	
3.4	Los datos del titular de la tarjeta no se almacenan en formato electrónico.

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 B (Sección 2), con fecha *(fecha de finalización del SAQ).*

Según los resultados observados en el SAQ B 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):***

☐	**En cumplimiento:** 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 **EN CUMPLIMIENTO**, y *(nombre de la empresa del comerciante)* ha demostrado un cumplimiento total con la PCI DSS.
☐	**Falta de cumplimiento:** 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 **FALTA DE CUMPLIMIENTO**, y *(nombre de la empresa del comerciante)* no ha demostrado un cumplimiento total con la PCI DSS. **Fecha objetivo** para el cumplimiento: 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. *Consulte con su adquiriente o la(s) marca(s) de pago antes de completar la Parte 4.*
☐	**En cumplimiento pero con una excepción legal:** 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. *Si está marcado, complete lo siguiente:*

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)

☐	El Cuestionario de autoevaluación B de las PCI DSS, Versión *(versión del SAQ)*, se completó de acuerdo con las instrucciones correspondientes.
☐	Toda la información dentro del arriba citado SAQ y en esta atestación representa razonablemente los resultados de mi evaluación en todos los aspectos sustanciales.
☐	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.
☐	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.
☐	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 3a. Reconocimiento de estado (cont.)	
☐	No existe evidencia de almacenamiento de datos completos de la pista[1], datos de CAV2, CVC2, CID, o CVV2[2], ni datos de PIN[3] después de encontrarse la autorización de la transacción en NINGÚN sistema revisado durante la presente evaluación.
☐	Los análisis del ASV completados por un Proveedor aprobado de escaneo (ASV) certificado por el PCI SSC *(nombre del ASV)*

Parte 3b. Declaración del comerciante	
Firma del director ejecutivo del comerciante ↗	*Fecha:*
Nombre del Oficial Ejecutivo del comerciante:	*Cargo:*

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:	

Firma del Oficial debidamente autorizado de la empresa del QSA ↗	*Fecha:*
Nombre del Oficial debidamente autorizado:	*Empresa de QSA:*

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:	

[1] 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.

[2] 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.

[3] 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 adquiriente 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	
3	Proteja los datos del titular de la tarjeta que fueron almacenados	☐	☐	
4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	☐	☐	
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.	☐	☐	
9	Restringir el acceso físico a los datos del titular de la tarjeta.	☐	☐	
12	Mantener una política que aborde la seguridad de la información para todo el personal	☐	☐	

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