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

Cuestionario de autoevaluación P2PE y Atestación de cumplimiento

Comerciantes que usan terminales de pago de hardware en una solución únicamente P2PE publicada por la PCI. Sin almacenamiento electrónico de 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
N/C	1.0		No utilizado
Mayo de 2012	2.0		Creación de un SAQ P2PE para comerciantes que utilizan solamente terminales de hardware como parte de una solución P2PE validada publicada por el PCI SSC. Este SAQ se utiliza con las 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*. Se eliminó "HW" del título del SAQ, ya que puede ser utilizado por los comerciantes que usan una solución HW/HW o HW/P2PE Híbrida.
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*. Se eliminaron los Requisitos 3.3 y 4.2 de PCI DSS, como se describe en la implementación de la solución PCI P2PE y PIM.
Enero de 2017	3.2	1.1	Cambios de documento actualizados para aclarar los requisitos eliminados en la actualización de abril de 2016.

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

Criterios de elegibilidad del comerciante para SAQ P2PE

SAQ P2PE se ha desarrollado para contemplar los requisitos aplicables a los comerciantes que procesan datos de los titulares de tarjetas solamente por medio de terminales de hardware incluidos en una solución de cifrado de punto a punto (P2PE) publicada y validada por la PCI.

Los comerciantes que corresponden al SAQ P2PE no tienen acceso a los datos de los titulares de tarjeta de texto claro en ningún sistema informático, y solamente ingresan los datos de la cuenta mediante terminales de pago de hardware desde una solución de P2PE aprobada por el PCI SSC. Los comerciantes que corresponden al SAQ P2PE pueden ser comerciantes con instalaciones físicas (con la tarjeta presente) o pedido por correo/teléfono (tarjeta no presente). Por ejemplo, un comerciante de pedido por correo/teléfono podría ser elegible para el SAQ P2PE si recibe datos de titulares de tarjetas en forma impresa o por teléfono, y los ingresa directa y únicamente en un dispositivo de hardware de P2PE validado.

Los comerciantes que corresponden al SAQ P2PE confirman que para este canal de pago:

- Todo el procesamiento de pagos se realiza a través de la solución de P2PE validada y aprobada por el PCI SSC;
- Los únicos sistemas en el entorno del comerciante que almacena, procesa o transmite los datos de cuenta son los dispositivos del punto de interacción (POI) que están aprobados para ser utilizados con la solución de P2PE publicada y validada por el PCI;
- Su empresa no recibe ni transmite de otro modo datos de titulares de tarjetas electrónicamente;
- No hay almacenamiento heredado de datos de titulares de tarjetas electrónicos en el entorno;
- Si su empresa almacena datos del titular de la tarjeta, estos solo están en informes impresos o copias de recibos impresos y no se reciben electrónicamente; **y**
- Su empresa implementó todos los controles en el *Manual de Instrucción de P2PE (PIM)* proporcionado por el proveedor de servicios de P2PE.

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.

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. Confirmar que implementó todos los elementos del PIM.
4. Evaluar su entorno respecto del cumplimiento con los requisitos aplicables de las PCI DSS.
5. 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 P2PE)

- 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)

6. Envíe el SAQ y la Atestación de cumplimiento (AOC), junto con cualquier otra documentación solicitada, a su adquirente, marca de pago u 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*. Completar todas las secciones. 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 empresa comerciante (marque todo lo que corresponda):		
☐ Comercio minorista	☐ Telecomunicaciones	☐ Tiendas de comestibles y supermercados
☐ Petróleo	☐ Pedidos por correo/teléfono	☐ 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. Solución de P2PE

Proporcione la siguiente información relativa a la solución PCI P2PE validada que su organización utiliza:

Nombre del proveedor de servicio de la solución de P2PE:	
Nombre de la solución de P2PE:	
Número de referencia del PCI SSC:	
Dispositivos POI P2PE en la lista usados por los Comerciantes (Dependencia de dispositivo PTS):	

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 proveedores de servicios externos (por ejemplo, Integrador o revendedor certificado (QIR), empresas de puertas de enlace, agentes de reservas en aerolíneas, agentes del programa de lealtad, etc.)? ***En caso de ser Sí:***	☐ Sí ☐ No

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

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

Parte 2g. Elegibilidad para completar el SAQ P2PE

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

☐	Todo el procesamiento de pagos se realiza a través de la solución de P2PE validada y aprobada por el PCI SSC (según lo anterior).
☐	Los únicos sistemas en el entorno del comerciante que almacena, procesa o transmite los datos de cuenta son los dispositivos del punto de interacción (POI) que están aprobados para ser utilizados con la solución de P2PE publicada por el PCI y validada.

Parte 2g. Elegibilidad para completar el SAQ P2PE	
El comerciante certifica que es elegible para completar esta versión abreviada del Cuestionario de autoevaluación porque, para este canal de pago:	
☐	El comerciante no recibe ni transmite de otro modo datos de titulares de tarjetas electrónicamente a través de canales.
☐	El comerciante verifica que no hay almacenamiento heredado de datos de titulares de tarjetas electrónicos en el entorno.
☐	Si el comerciante almacena datos del titular de la tarjeta, estos solo están en informes impresos o copias de recibos impresos y no se reciben electrónicamente, **y**.
☐	El comerciante implementó todos los controles en el Manual de Instrucción de P2PE (PIM) proporcionado por el proveedor de servicios de P2PE.

Sección 2: Cuestionario de autoevaluación P2PE

Nota: *Las siguientes preguntas están numeradas de acuerdo con los requisitos y procedimientos de prueba reales de las PCI DSS, tal como se definen en el documento de los* Procedimientos de evaluación de seguridad y requisitos de las PCI DSS*. Dado que solamente un subconjunto de los requisitos de las PCI DSS se proporciona en este SAQ P2PE, la numeración de estas preguntas puede no ser consecutiva.*

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

Nota: *El Requisito 3 se aplica solamente a los comerciantes que corresponden al SAQ P2PE que tienen registros impresos (por ejemplo, recibos, informes impresos, etc.) con datos de cuentas, incluidos los números de cuenta principales (Primary Account Numbers, PAN).*

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
3.1	¿Están implementados los procedimientos, los procesos y las políticas para la retención y eliminación de datos de la siguiente manera?					
	(a) ¿Está el período de almacenamiento de datos y el tiempo de retención limitado a la cantidad exigida por los requisitos legales, reglamentarios y del negocio?	▪ Revisar los procedimientos y las políticas de retención y eliminación de datos ▪ Entrevistar al personal	☐	☐	☐	☐
	(b) ¿Hay implementados procesos definidos que permitan la eliminación segura de datos de titulares de tarjetas cuando ya no son necesarios por motivos legales, reglamentarios o del negocio?	▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Examinar los mecanismos de eliminación	☐	☐	☐	☐
	(c) ¿Existen requisitos específicos de retención para los datos de titulares de tarjetas? *Por ejemplo, los datos de los titulares de tarjetas que se retendrán durante un período X por razones de negocio.*	▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Examinar los requisitos de retención	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
	(d) ¿Existe un proceso trimestral para la identificación y eliminación, de manera segura, de los datos del titular de la tarjeta almacenados que excedan los requisitos de retención definidos?	▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Observar los procesos de eliminación	☐	☐	☐	☐
	(e) ¿Reúnen todos los datos de titulares de tarjetas los requisitos definidos en la política de retención de datos?	▪ Examinar los archivos y los registros del sistema	☐	☐	☐	☐
Guía: *Las respuestas "Sí" para los requisitos 3.1 significan que si un comerciante almacena cualquier tipo de papel (por ejemplo, recibos o informes impresos) que contiene datos de la cuenta, el comerciante solamente lo almacena por el término que sea necesario según razones comerciales, legales o reguladoras, y lo destruye una vez que ya no es más necesario.* *Si un comerciante nunca imprime ni almacena papel que contenga datos de cuenta, debe marcar la columna "N/C" y completar la hoja de trabajo "Explicación de no aplicabilidad" en el Anexo C.*						
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) para todo el almacenamiento de papel?	▪ Examinar fuentes de datos en papel	☐	☐	☐	☐
Guía: *Una respuesta "Sí" para el Requisito 3.2.2 significa que si el comerciante escribe el código de seguridad de la tarjeta mientras se realiza la transacción, luego destruye el papel en forma segura (por ejemplo, con un triturador de papel) de inmediato una vez realizada la transacción, u oscurece el código (por ejemplo, al "tacharlo" con un marcador negro) antes de almacenar el papel.* *Si un comerciante nunca solicita el número de tres o cuatro cifras impreso en el frente o el dorso de una tarjeta de pago ("código de seguridad de la tarjeta"), debe marcar la columna "N/C" y completar la hoja de trabajo "Explicación de no aplicabilidad" en el Anexo C.*						

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	**Sí con CCW**	**No**	**N/C**
3.7	¿Las políticas de seguridad y los procedimientos operativos para la protección de los datos de titulares de tarjetas ▪ están documentados? ▪ están en uso? ▪ son de conocimiento para todas las partes afectadas?	▪ Revisar las políticas y los procedimientos operativos de seguridad ▪ Entrevistar al personal	☐	☐	☐	☐
Guía: *Una respuesta "Sí" para el Requisito 3.7 significa que, si el comerciante tiene almacenamiento en papel de los datos de la cuenta, cuenta con las políticas y los procedimientos implementados para los Requisitos 3.1, 3.2.2 y 3.3. Esto ayuda a asegurar que el personal conoce y respeta las políticas de seguridad y los procedimientos operativos documentados para administrar, de manera segura, el almacenamiento continuo de los datos del titular de la tarjeta.*						

Implementar medidas sólidas de control de acceso

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

Nota: *Los requisitos 9.5 y 9.8 se aplican solamente a los comerciantes correspondientes al SAQ P2PE que tienen registros impresos (por ejemplo, recibos, informes impresos, etc.) con datos de cuentas, incluidos los números de cuenta principales (PAN)*

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	☐	☐	☐	☐
9.8	(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 se transforman en 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	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
Guía: *Las respuestas "Sí" a los requisitos en 9.5 y 9.8 significan que si un comerciante almacena en forma segura cualquier tipo de papel que contiene datos de la cuenta, por ejemplo, los almacena en un cajón o gabinete con cerradura, o en una caja fuerte y lo destruye una vez que ya no es más necesario a los fines comerciales. En esto se incluye una política o documento escrito para los empleados, de manera que sepan cómo asegurar el papel con datos de cuenta y cómo destruir el papel cuando ya no se lo necesita más.* *Si un comerciante nunca almacena papel que contenga datos de cuenta, debe marcar la columna "N/C" y completar la hoja de trabajo "Explicación de no aplicabilidad" en el Anexo C.*						
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	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
9.9.3	¿Está capacitado el personal para que detecten indicios de alteración o sustitución en los dispositivos?					
	(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	☐	☐	☐	☐

Guía: *Las respuestas "Sí" a los Requisitos en 9.9 significan que el comerciante tiene políticas y procedimientos implementados para los Requisitos 9.9.1-9.9.3, y que mantiene una lista actualizada de dispositivos, realiza inspecciones de estos en forma periódica y capacita a los empleados respecto de a qué deben estar atentos para detectar dispositivos alterados o reemplazados.*

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
9.10	¿Las políticas de seguridad y los procedimientos operativos para la restricción del acceso físico a los datos de titulares de tarjetas ▪ están documentados? ▪ están en uso? ▪ son de conocimiento para todas las partes afectadas?	▪ Examinar las políticas de seguridad y los procedimientos operativos ▪ Entrevistar al personal	☐	☐	☐	☐
Guía: *Una respuesta "Sí" al Requisito 9.10 significa que el comerciante tiene las políticas y los procedimientos implementados para los Requisitos 9.5, 9.8 y 9.9, según corresponde por el entorno. Esto ayuda a asegurar que el personal conoce y respeta las políticas de seguridad y los procedimientos operativos documentados.*						

Mantener una política de seguridad de información

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

Nota: En el Requisito 12 se especifica que los comerciantes deben tener políticas de seguridad de la información implementadas para sus empleados, pero la sencillez o complejidad de dichas políticas es relativa al tamaño y la complejidad de las operaciones del comerciante. Se debe proporcionar el documento de política a todo el personal para que tomen conciencia de sus responsabilidades para proteger los terminales de pago y los documentos impresos con datos del titular de la tarjeta, etc. Si un comerciante no tiene empleados, entonces se espera que el comerciante entienda y reconozca su responsabilidad de la seguridad dentro de su tienda(s).

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	☐	☐	☐	☐
Guía: *Las respuestas "Sí" a los requisitos en 12.1 significan que el comerciante debe tener una política razonable para el tamaño y la complejidad de las operaciones del comerciante, y que se la revisa en forma anual y se la actualiza de ser necesario. Por ejemplo, una política tal podría ser un documento sencillo que abarque la manera en que debe proteger la tienda y los dispositivos de pago de acuerdo con el* Manual de Instrucción de P2PE (PIM), *y a quién se debe llamar en caso de emergencia.*						
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	☐	☐	☐	☐
Guía: *Una respuesta "Sí" al Requisito 12.4 significa que la política de seguridad del comerciante define las responsabilidades de seguridad fundamentales para todos los empleados, de acuerdo con el tamaño y la complejidad de las operaciones del comerciante. Por ejemplo, las responsabilidades de seguridad pueden definirse de acuerdo con las responsabilidades fundamentales según los niveles de los empleados, como las responsabilidades que se esperan que asuma un gerente o un propietario, y aquellas de los empleados administrativos.*						
12.5	¿Las siguientes responsabilidades de administración de seguridad de la información están asignadas a una persona o equipo?					

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
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	☐	☐	☐	☐
Guía: *Una respuesta "Sí" al Requisito 12.5.3 significa que el comerciante cuenta con una persona designada como responsable de la respuesta ante incidentes y del plan de escalación que se exigen en 12.9.*						
12.6	(a) ¿Se ha implementado un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de los procedimientos y la política de seguridad de los datos del titular de la tarjeta?	▪ Revisar el programa de concienciación sobre seguridad	☐	☐	☐	☐
Guía: *Una respuesta "Sí" al Requisito 12.6 significa que el comerciante cuenta con un programa de concienciación de seguridad implementado, que es coherente con el tamaño y la complejidad de las operaciones del comerciante. Por ejemplo, un programa de concienciación sencillo puede ser un boletín informativo publicado en la oficina administrativa, o el envío periódico de correos electrónicos a todos los empleados. Entre los ejemplos de mensajes como programa de concienciación se incluyen las descripciones de recomendaciones de seguridad que todos los empleados deben respetar, como el cierre de las puertas y los recipientes de almacenamiento, cómo determinar si se alteró un terminal de pago, y cómo identificar a los empleados legítimos que podrían utilizar los terminarles de pago de hardware.*						
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	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
Guía: *Las respuestas "Sí" a los requisitos en 12.8 significan que el comerciante tiene una lista de proveedores de servicios con quienes mantiene acuerdos, además de compartir datos de titulares de tarjetas. Por ejemplo, dichos acuerdos serían aplicables si un comerciante usa una empresa de retención de documentos para almacenar documentación impresa que incluye datos de cuenta.*						
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	☐	☐	☐	☐
Guía: *Las respuestas "Sí" a los requisitos en 12.10 significan que el comerciante cuenta con un plan de escalación y respuesta ante incidentes documentado que debe usarse en caso de emergencia, que es coherente con el tamaño y la complejidad de las operaciones del comerciante. Por ejemplo, un plan semejante podría ser un documento sencillo publicado en la oficina administrativa que enumera los contactos a los que debe llamarse en las diversas situaciones, con una revisión anual para confirmar que continúa siendo actual, pero también podría ser incluir un plan de respuesta ante incidentes completo, con información sobre instalaciones de "sitio caliente" de respaldo y una prueba anual exhaustiva. Este plan debe estar al alcance de todos los empleados para utilizar como recurso en una emergencia.*						

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 SAQ P2PE.

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:	
12.8	Los datos de los titulares de tarjetas nunca se comparten con los proveedores de servicios.

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 P2PE (Sección 2), con fecha *(fecha de finalización del SAQ).*

Según los resultados observados en el SAQ P2PE 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 P2PE de las PCI DSS y se ha respondido afirmativamente a todas las preguntas, lo que resulta en una calificación general de **EN CUMPLIMIENTO**, y de esta manera *(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 P2PE de las 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 de esta manera *(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, ya que no todas las marcas de pago necesitan esta sección.*
☐	**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 P2PE de las PCI DSS, Versión *(versión del SAQ)*, se completó de acuerdo con las instrucciones correspondientes.
☐	Toda la información dentro del anteriormente citado SAQ y en esta declaración representa razonablemente los resultados de mi evaluación en todos los aspectos sustanciales.
☐	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.

Parte 3a. Reconocimiento de estado (cont.)	
☐	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.
☐	No existe evidencia de datos completos de la pista[1], datos de CAV2, CVC2, CID, o CVV2[2], ni datos de PIN[3] en NINGÚN sistema revisado durante la presente evaluación.

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. Las entidades no pueden retener todos los datos de la 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.

[2] El valor de tres o cuatro dígitos impreso sobre o a la derecha del 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 el estado “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, ya que no todas las marcas de pago necesitan esta sección.

Requisito de las PCI DSS*	**Descripción del requisito**	**En cumplimiento con los requisitos de las PCI DSS** (seleccione una opción)		**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	☐	☐	
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.*