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

Cuestionario de Autoevaluación C-VT y Declaración de Cumplimiento

Comerciantes con terminales de pago virtuales basadas en la Web – Sin almacenamiento electrónico de datos de 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 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 *PCI DSS – Resumen de cambios de las PCI DSS versión 3.1 a 3.2*. Requisitos añadidos de PCI DSS v3.2 Requisitos 8, 9 y Apéndice A2.
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 los sistemas permitidos. Se agregó el requisito 8.3.1 para alinearse con la intención del requisito 2.3. Se agregó el requisito 11.3.4 para verificar los controles de segmentación, si se utiliza la segmentación.

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

SAQ C-VT se ha desarrollado para contemplar los requisitos aplicables a los comerciantes que procesan datos de los titulares de tarjetas solamente por medio de terminales virtuales aislados en computadoras personales conectadas a Internet.

Un terminal de pago virtual es un acceso basado en explorador web para un adquiriente, procesador o sitio web de proveedor de servicios externos que permite autorizar transacciones de tarjetas de pago, donde el comerciante ingresa manualmente datos de tarjetas de pago mediante un explorador web conectado de forma segura. A diferencia de los terminales físicos, los terminales de pago virtuales no leen datos directamente de una tarjeta de pago. Debido a que las transacciones de tarjetas de pago se ingresan manualmente, comúnmente se utilizan terminales de pago virtuales en lugar de terminales físicos en entornos de comerciantes con bajo volumen de transacciones.

Los comerciantes que corresponden al SAQ C-VT procesan datos de titulares de tarjetas solo a través de un terminal de pago virtual y no almacenan los datos de titulares de tarjetas en ningún sistema informático. Estos terminales virtuales están conectados a Internet para acceder a un tercero que hospeda la función de procesamiento de pagos en terminales virtuales. Este tercero puede ser un procesador, adquiriente u otro proveedor de servicios externo que almacena, procesa y/o transmite los datos de los titulares de tarjetas para autorizar y/o liquidar las transacciones de pago en terminal virtual de los comerciantes.

Esta opción de SAQ está dirigida solo a comerciantes que ingresan manualmente una sola transacción a la vez utilizando un teclado en una solución de terminal virtual basado en Internet. Los comerciantes que se corresponden al SAQ C-VT pueden ser comerciantes con instalaciones físicas (con la tarjeta presente) o pedido por correo/teléfono (tarjeta no presente).

Los comerciantes correspondientes al SAQ C-VT confirman que para este canal de pago:

- El único procesamiento de pagos de su empresa se realiza a través de un terminal de pago virtual al que se accede mediante un explorador web conectado a Internet;
- La solución de terminal de pago virtual de su empresa está proporcionada y hospedada por un proveedor de servicios externo validado por las PCI DSS;
- Su empresa accede a la solución de terminal de pago virtual compatible con las PCI DSS a través de una computadora que está aislada en una ubicación individual, y no está conectada a otras ubicaciones ni sistemas dentro de su entorno (esto se puede lograr mediante un firewall o una segmentación de red para aislar la computadora de los demás sistemas)[1];
- La computadora de su empresa no tiene software instalado que ocasione que los datos de titulares de tarjetas se almacenen (por ejemplo, no hay software para procesamiento por lotes o almacenamiento y transmisión);
- La computadora de su empresa no tiene dispositivos de hardware conectados que se utilizan para capturar o almacenar datos de titulares de tarjetas (por ejemplo, no hay lectores de tarjetas conectados);

[1] Este criterio no pretende prohibir que más de un equipo del tipo de sistema permitido (es decir, un terminal de pago virtual accedido por un navegador web conectado a Internet) se encuentre en la misma zona de red, siempre que los sistemas permitidos estén aislados de otros tipos de sistemas (por ejemplo, mediante la implementación de la segmentación de red). Además, este criterio no pretende impedir que el tipo de sistema definido pueda transmitir la información de la transacción a un tercero para su procesamiento, tal como un adquirente o procesador de pago, a través de una red.

- Su empresa no recibe de otro modo datos de titulares de tarjetas electrónicamente a través de canales (por ejemplo, mediante una red interna o 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 C-VT)
    - 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 bien muchas de las organizaciones que completan el SAQ C-VT deberán validar su cumplimiento con todos los requisitos de las PCI DSS establecidos en este SAQ, es posible que algunas de las organizaciones con modelos de negocio muy específicos encuentren que algunos requisitos no son aplicables. Por ejemplo, no se esperaría de una compañía que no utiliza tecnología inalámbrica en modo alguno que valide el cumplimiento con las secciones de las PCI DSS relacionadas con el manejo de tecnología inalámbrica (por ejemplo, Requisitos 1.2.3, 2.1.1, y 4.1.1).

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) ☐ Comercio electrónico ☐ Tarjeta presente (en persona)	☐ 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 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 C-VT

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

☐	El único procesamiento de pagos del comerciante se realiza a través de un terminal de pago virtual al que se accede mediante un explorador web conectado a Internet;
☐	La solución de terminal de pago virtual del comerciante está proporcionada y hospedada por un proveedor de servicios externo validado por las PCI DSS;

☐	El comerciante accede al terminal virtual que cumple con las PCI DSS mediante una computadora aislada en una ubicación individual que no está conectada a otras ubicaciones ni sistemas dentro de su entorno;
☐	La computadora del comerciante no tiene software instalado que ocasione que los datos de titulares de tarjetas se almacenen (por ejemplo, no hay software para procesamiento por lotes o almacenamiento y transmisión);
☐	La computadora del comerciante no tiene dispositivos de hardware conectados que se utilizan para capturar o almacenar datos de titulares de tarjetas (por ejemplo, no hay lectores de tarjetas conectados);
☐	El comerciante no recibe de otro modo datos de titulares de tarjetas electrónicamente a través de canales (por ejemplo, mediante una red interna o 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 C-VT

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 1: Instalar y mantener una configuración de firewall para proteger los datos

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
1.2	¿Restringen las configuraciones para firewalls y routers las conexiones entre redes no confiables y cualquier sistema en el entorno de los datos de titulares de tarjeta de la manera siguiente? ***Nota:*** *Una "red no confiable" es toda red externa a las redes que pertenecen a la entidad en evaluación o que excede la capacidad de control o administración de la entidad.*					
1.2.1	(a) ¿Está restringido el tránsito entrante y saliente a la cantidad necesaria para el entorno de los datos de titulares de tarjetas?	▪ Revisar las normas de configuración del firewall y el router ▪ Examinar las configuraciones de firewalls y routers	☐	☐	☐	☐
	(b) ¿Se niega todo el resto del tránsito entrante o saliente (por ejemplo, mediante la utilización de una declaración explícita "negar todos" o una negación implícita después de una declaración de permiso)?	▪ Revisar las normas de configuración del firewall y el router ▪ Examinar las configuraciones de firewalls y routers	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
1.2.3	¿Hay firewalls de perímetro instalados entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y están estos firewalls configurados para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta?	▪ Revisar las normas de configuración del firewall y el router ▪ Examinar las configuraciones de firewalls y routers	☐	☐	☐	☐
1.3	¿Se prohíbe el acceso directo público entre Internet y cualquier componente del sistema en el entorno de datos de los titulares de tarjetas de la manera siguiente?					
1.3.4	¿Está el tráfico saliente desde el entorno de datos del titular de la tarjeta a Internet expresamente autorizado?	▪ Examinar las configuraciones de firewalls y routers	☐	☐	☐	☐
1.3.5	¿Solo se permite la entrada a la red de conexiones establecidas?	▪ Examinar las configuraciones de firewalls y routers	☐	☐	☐	☐
1.4	(a) ¿Hay instalado en forma activa software de firewall personal (o una funcionalidad equivalente) en todos los dispositivos móviles (incluidos los de propiedad de los trabajadores y/o de la empresa) que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usan para acceder al CDE?	▪ Revisar las normas de configuración y las políticas ▪ Examinar los dispositivos móviles y/o propiedad de los empleados	☐	☐	☐	☐
	(b) ¿Está configurado el software de firewall personal (o una funcionalidad equivalente) con parámetros de configuración específicos, en funcionamiento activo y de forma tal que los usuarios de dispositivos móviles o de propiedad de trabajadores no puedan alterarlo?	▪ Revisar las normas de configuración y las políticas ▪ Examinar los dispositivos móviles y/o propiedad de los empleados	☐	☐	☐	☐

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? *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.*	▪ Revisar las políticas y los procedimientos ▪ Examinar la documentación del proveedor ▪ Observar las configuraciones del sistema y las configuraciones de cuenta ▪ Entrevistar al personal	☐	☐	☐	☐
	(b) ¿Se eliminan o desactivan las cuentas predeterminadas que no son necesarias antes de instalar un sistema en la red?	▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema y las configuraciones de cuenta ▪ Entrevistar al personal	☐	☐	☐	☐
2.1.1	Para entornos con tecnología inalámbrica conectados al entorno de datos del titular de la tarjeta o a la transmisión de datos de los titulares de tarjeta, ¿se cambian los valores predeterminados de la siguiente manera?					
	(a) ¿Se cambian las claves de cifrado predeterminadas al momento de la instalación, y se cambian cada vez que una persona que tenga conocimiento de éstas cesa en sus funciones o se traslada a otro cargo en la empresa?	▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ 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
	(b) ¿Se cambian las cadenas comunitarias SNMP predeterminadas en los dispositivos inalámbricos en la instalación?	▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Entrevistar al personal ▪ Examinar las configuraciones del sistema				
	(c) ¿Se cambian las contraseñas/frases de contraseña predeterminadas en los puntos de acceso en la instalación?	▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
	(d) ¿Se actualiza el firmware de los dispositivos inalámbricos a los efectos de admitir el cifrado sólido para la autenticación y la transmisión en redes inalámbricas?	▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
	(e) ¿Se cambian otros valores de seguridad de sistemas inalámbricos predeterminados por los proveedores, si corresponde?	▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
2.2.2	(a) ¿Solo los servicios necesarios, protocolos, daemons, etc. son habilitados según lo exija la función del sistema (los servicios y protocolos que no sean directamente necesarios para desempeñar la función especificada del dispositivo están inhabilitados)?	▪ Revisar las normas de configuración ▪ Examinar las configuraciones del sistema	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
	(b) ¿Están todos los servicios, daemons o protocolos habilitados que no son seguros justificados de conformidad con las normas de configuración documentadas?	▪ Revisar las normas de configuración ▪ Entrevistar al personal ▪ Examinar los parámetros de configuración ▪ Comparar los servicios habilitados, etc. con las justificaciones documentadas	☐	☐	☐	☐
2.2.3	¿Están implementadas y documentadas las funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros? ***Nota:*** *Cuando se utiliza SSL/TLS temprana, deben completarse los requisitos establecidos en el Anexo A2.*	▪ Revisar las normas de configuración ▪ Examinar los parámetros de configuración	☐	☐	☐	☐
2.2.4	(a) ¿Tienen conocimiento los administradores del sistema y/o el personal que configura los componentes del sistema de los parámetros de configuración de seguridad comunes correspondientes a dichos componentes del sistema?	▪ Entrevistar al personal	☐	☐	☐	☐
	(b) ¿Están incluidos los parámetros de configuración de seguridad del sistema en las normas de configuración de sistemas?	▪ Revisar las normas de configuración del sistema	☐	☐	☐	☐
	(c) ¿Se configuraron apropiadamente los parámetros de seguridad en los componentes del sistema?	▪ Examinar los componentes del sistema ▪ Examinar la configuración de los parámetros de seguridad ▪ Comparar la configuración con las normas de configuración del sistema	☐	☐	☐	☐
2.2.5	(a) ¿Se eliminaron todas las funcionalidades innecesarias, tales como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios?	▪ Examinar los parámetros de seguridad en 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
	(b) ¿Se documentaron todas las funciones habilitadas y admiten estas una configuración segura?	▪ Revisar la documentación ▪ Examinar los parámetros de seguridad en los componentes del sistema	☐	☐	☐	☐
	(c) ¿Están presentes en los componentes del sistema solo las funcionalidades documentadas?	▪ Revisar la documentación ▪ Examinar los parámetros de seguridad en los componentes del sistema	☐	☐	☐	☐
2.3	¿Se cifró el acceso administrativo que no es de consola de la siguiente manera? ***Nota:*** *Cuando se utiliza SSL/TLS temprana, deben completarse los requisitos establecidos en el Anexo A2.*					
	(a) ¿La totalidad del acceso administrativo que no es de consola se cifra con criptografía sólida, y se invoca un método de cifrado sólido antes de que se solicite una contraseña de administrador?	▪ Examinar los componentes del sistema ▪ Examinar las configuraciones del sistema ▪ Observar a un administrador mientras se conecta	☐	☐	☐	☐
	(b) ¿Los servicios del sistema y los archivos de parámetros son configurados de modo que impidan el uso de Telnet y otros comandos de inicio de sesión remotos inseguros?	▪ Examinar los componentes del sistema ▪ Examinar servicios y archivos	☐	☐	☐	☐
	(c) ¿El acceso de administradores a la interfaz de administración basada en la web está cifrado mediante una sólida criptografía?	▪ Examinar los componentes del sistema ▪ Observar a un administrador mientras se conecta	☐	☐	☐	☐
	(d) En el caso de la terminología en uso, ¿se encuentra implementada una criptografía de acuerdo con las mejores prácticas de la industria y las recomendaciones del proveedor?	▪ Examinar los componentes del sistema ▪ Revisar la documentación del proveedor ▪ Entrevistar al personal	☐	☐	☐	☐

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)?					
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	☐	☐	☐	☐
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	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
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
4.1	(a) ¿Se utilizan criptografía y protocolos de seguridad sólidos para salvaguardar datos confidenciales de titulares de tarjetas durante su transmisión a través de redes públicas abiertas? ***Nota:*** *Cuando se utiliza SSL/TLS temprana, deben completarse los requisitos establecidos en el Anexo A2.* *Ejemplos de redes públicas abiertas son Internet, las tecnologías inalámbricas, incluidas 802.11 y Bluetooth; las tecnologías celulares, por ejemplo, el sistema global de comunicaciones móviles (GSM), el acceso múltiple por división de código (CDMA) y el servicio de radio por paquetes generales (GPRS).*	▪ Revisar las normas documentadas ▪ Revisar las políticas y los procedimientos ▪ Revisar todas las ubicaciones donde se transmiten o reciben datos del titular de la tarjeta ▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
	(b) ¿Solo se aceptan claves/certificados de confianza?	▪ Observar las transmisiones entrantes y salientes ▪ Examinar claves y certificados de confianza	☐	☐	☐	☐
	(c) ¿Hay implementados protocolos de seguridad para utilizar solo configuraciones seguras y no admitir versiones o configuraciones inseguras?	▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
	(d) ¿Se implementa el nivel de cifrado adecuado para la metodología de cifrado que se utiliza (ver recomendaciones de proveedores/mejores prácticas)?	▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
	(e) Para las implementaciones de TLS, ¿está TLS habilitado al transmitir o recibir los datos del titular de la tarjeta? *Por ejemplo, para implementaciones basadas en explorador web:* • *"HTTPS" aparece como el protocolo URL (Universal Record Locator).* • *Los datos del titular de la tarjeta solo se solicitan si "HTTPS" aparece como parte del URL.*	▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
4.1.1	¿Se aplican las mejores prácticas de la industria para implementar el cifrado sólido para la autenticación y transmisión para redes inalámbricas de transmisión de datos de los titulares de tarjeta o conectados con el entorno de datos del titular de la tarjeta?	▪ Revisar las normas documentadas ▪ Revisar redes inalámbricas ▪ Examinar los parámetros de configuración del sistema	☐	☐	☐	☐
4.2	(b) ¿Se implementaron políticas que especifiquen que no se deben enviar números PAN sin protección a través de tecnologías de mensajería del usuario final?	▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐

Mantener un programa de administración de vulnerabilidad

Requisito 5: Proteger todos los sistemas de malware y actualizar los programas o software antivirus regularmente

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
5.1	¿Se instala software anti-virus en todos los sistemas comúnmente afectados por software malicioso?	▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
5.1.1	¿Todos los programas antivirus son capaces de detectar, eliminar y proteger contra todos los tipos conocidos de software malicioso (por ejemplo, virus, troyanos, gusanos, spyware, adware y rootkit)?	▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema	☐	☐	☐	☐
5.1.2	¿Se realizan evaluaciones habituales para identificar y evaluar las amenazas de malware en evolución de manera de poder confirmar si aquellos sistemas que no suelen verse afectados por programas de software maliciosos se mantienen así?	▪ Entrevistar al personal	☐	☐	☐	☐
5.2	¿Todos los mecanismos de antivirus cumplen con lo siguiente?					
	(a) ¿Están actualizados el software antivirus y las definiciones?	▪ Examinar las políticas y los procedimientos ▪ Examinar las configuraciones de antivirus, incluida la instalación maestra ▪ Examinar los componentes del sistema	☐	☐	☐	☐
	(b) ¿Están habilitados los análisis periódicos y las actualizaciones automáticas, y se los realiza?	▪ Examinar las configuraciones de antivirus, incluida la instalación maestra ▪ Examinar 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
	(c) ¿Están todos los mecanismos anti-virus generando registros de auditoría, y ¿son conservados los registros de conformidad con el Requisito 10.7 de las PCI DSS?	▪ Examinar las configuraciones de antivirus ▪ Revisar los procesos de retención de registros	☐	☐	☐	☐
5.3	¿Todos los mecanismos antivirus ▪ están funcionando activamente? ▪ ¿Los mecanismos antivirus no pueden ser deshabilitados ni alterados por usuarios? ***Nota:*** *Las soluciones antivirus pueden desactivarse temporalmente, pero solo si existe una necesidad técnica legítima autorizada por la gerencia con un criterio casuístico. Si es necesario desactivar la protección antivirus por un motivo específico, debe contarse con una autorización formal. Podría ser necesario implementar medidas de seguridad adicionales para el período en que no esté activa la protección antivirus.*	▪ Examinar las configuraciones de antivirus ▪ Examinar los componentes del sistema ▪ Observar los procesos ▪ Entrevistar al personal	☐	☐	☐	☐

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
6.1	¿Existe un proceso para identificar vulnerabilidades de seguridad, incluida la siguiente? ▪ ¿Usar fuentes externas conocidas para obtener información sobre las vulnerabilidades? ▪ ¿Asignar una clasificación de riesgo a las vulnerabilidades en la que se identifiquen todas las vulnerabilidades de “alto riesgo” y “críticas”? ***Nota**: Las clasificaciones de riesgo deben basarse en las mejores prácticas de la industria y en la posible incidencia. Por ejemplo, en los criterios para clasificar las vulnerabilidades, se puede tener en cuenta la puntuación base CVSS, la clasificación del proveedor o el tipo de sistema afectado.* *Los métodos para evaluar las vulnerabilidades y asignar las clasificaciones de riesgo varían según el entorno y la estrategia de evaluación de riesgos de la organización, Las clasificaciones de riesgo deben identificar, mínimamente, todas las vulnerabilidades que se consideren de “alto riesgo” para el entorno. Además de la clasificación de riesgos, las vulnerabilidades se pueden considerar “críticas” si suponen una amenaza inminente para el entorno, si afectan los sistemas o si generan un posible riesgo si no se contemplan. Algunos ejemplos de sistemas críticos son los sistemas de seguridad, los dispositivos y sistemas públicos, las bases de datos y otros sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta.*	▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Observar los procesos	☐	☐	☐	☐
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?	▪ 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
	(b) ¿Se instalan parches de seguridad crítica en un lapso de un mes contado a partir de su fecha de lanzamiento? ***Nota**: Los parches de seguridad críticos deben identificarse de conformidad con el proceso de clasificación de riesgos definido en el Requisito 6.1.*	▪ Revisar las políticas y los procedimientos ▪ Examinar los componentes del sistema ▪ Comparar la lista de los parches de seguridad instalados con las listas de parches de proveedor recientes	☐	☐	☐	☐

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	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
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 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?	▪ Revisar los procedimientos de contraseña ▪ Entrevistar al personal	☐	☐	☐	☐
8.1.3	¿Se desactiva o elimina de manera inmediata el acceso de cualquier usuario cesante?	▪ Revisar los procedimientos de contraseña ▪ Examinar las cuentas de usuarios cesantes ▪ Revisar las listas de acceso actuales ▪ Observar los dispositivos de autenticación física devueltos	☐	☐	☐	☐
8.2	¿Además de asignar una ID única, se emplean uno o más de los siguientes métodos para autenticar a todos los usuarios? ▪ Algo que el usuario sepa, como una contraseña o frase de seguridad ▪ Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente ▪ Algo que el usuario sea, como un rasgo biométrico	▪ Revisar los procedimientos de contraseña ▪ Observar los procesos de autenticación	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
8.2.3	(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? • Longitud de contraseña mínima de siete caracteres • Combinación de caracteres numéricos y alfabéticos De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.	▪ Examinar los parámetros de configuración del sistema para verificar los parámetros de la contraseña	☐	☐	☐	☐
8.3	Se asegura todo el acceso administrativo sin consola individual y todo el acceso remoto al CDE usando la autenticación de múltiples factores, como sigue: ***Nota:*** *La autenticación de múltiples factores exige utilizar dos de los tres métodos de autenticación (consulte el Requisito 8.2 de las PCI DSS para obtener una descripción de los métodos de autenticación). El uso de un mismo factor dos veces (por ejemplo, utilizar dos contraseñas individuales) no se considera una autenticación de múltiples factores.*					
8.3.1	¿Se incorpora la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE para el personal con acceso administrativo? ***Nota:*** *Este requisito se considerará una mejor práctica hasta el 31 de enero de 2018, momento a partir del cual se convertirá en requisito.*	▪ Examinar las configuraciones del sistema ▪ Observar el inicio de sesión del administrador en CDE	☐	☐	☐	☐

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? ▪ Las ID de usuario y cuentas genéricas se inhabilitan o eliminan; ▪ No existen las ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas; y ▪ ¿No se utilizan las identificaciones de usuario compartidas y genéricas para administrar componentes del sistema?	▪ Revisar las políticas y los procedimientos ▪ Examinar las listas de identificaciones de usuario ▪ Entrevistar al personal	☐	☐	☐	☐

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
9.1	¿Existen controles apropiados de entrada a la empresa para limitar y supervisar el acceso físico a sistemas en el entorno de datos de titulares de tarjetas?	▪ Observar los controles de acceso físicos ▪ Observar al personal	☐	☐	☐	☐
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	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
9.7	¿Se lleva un control estricto sobre el almacenamiento y accesibilidad de los medios?	▪ Revisar las políticas y los procedimientos	☐	☐	☐	☐
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 medios 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	☐	☐	☐	☐

Supervisar y evaluar las redes con regularidad

Requisito 11: Probar periódicamente los sistemas y procesos de seguridad

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	Sí con CCW	No	N/C
11.3.4	Si se usa la segmentación para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes:					
	(a) ¿Están definidos los procedimientos de las pruebas de penetración para comprobar todos los métodos de segmentación y confirmar que son operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los CDE?	▪ Examinar los controles de segmentación ▪ Revisar la metodología de pruebas de penetración	☐	☐	☐	☐
	(b) ¿Las pruebas de penetración para verificar los controles de segmentación cumplen con lo siguiente? • Se realizan, al menos, una vez al año y después de cualquier cambio en los controles o métodos de segmentación. • Abarcan todos los controles o métodos de segmentación implementados. • Verifica que los métodos de segmentación sean operativos y eficaces, y que aíslan todos los sistemas fuera de alcance de los CDE.	▪ Examinar los resultados de la prueba de penetración más reciente	☐	☐	☐	☐
	(c) ¿Las pruebas son realizadas por un recurso interno calificado o por un tercero calificado y, si corresponde, la empresa que realiza las pruebas garantiza la independencia organizativa? (no es necesario que sea un QSA o ASV).	▪ Entrevistar al personal a cargo	☐	☐	☐	☐

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 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 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 adicionales de las PCI DSS para las entidades que utilizan SSL/TLS **temprana***

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	**Sí con CCW**	**No**	**N/C**
A2.1	*Para los terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) utilizando SSL y/o TLS temprana:* • Se confirmaron los dispositivos para que no sean susceptibles a ninguna explotación conocida para SSL/TLS temprana *O bien:* • ¿Hay un Plan de migración y de Mitigación de riesgo formal implementado según el Requisito A2.2?	▪ Revisar la documentación (por ejemplo, documentación del proveedor, detalles de configuración del sistema/red, etc.) que verifique que los dispositivos POS POI no son susceptibles a ninguna vulnerabilidad conocida para SSL/TLS temprana.	☐	☐	☐	☐

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta *(Marque únicamente una respuesta para cada pregunta)*			
			Sí	**Sí con CCW**	**No**	**N/C**
A2.2	Hay un Plan de migración y de Mitigación de riesgo formal implementado para todas las implementaciones que usan SSL y/o TLS temprana (que no sea lo permitido en el Requisito A2.1), que incluya: ▪ Descripción del uso, incluidos los datos que se están transmitiendo, los tipos y el número de sistemas que utilizan y/o dan soporte a SSL/TLS temprana, el tipo de entorno; ▪ Los resultados de la evaluación de riesgos y los controles de reducción de riesgos están implementados; ▪ Descripción de los procesos a monitorear para las nuevas vulnerabilidades asociadas con SSL/TLS temprana; ▪ Descripción de los procesos de control de cambios que se implementan para garantizar que SSL/TLS temprana no se implementa en los nuevos entornos; ▪ ¿El resumen del plan de proyecto de migración incluye la fecha de finalización de la migración objetivo no más tarde del 30 de junio de 2018?	▪ Revisar el Plan de migración y de Mitigación de riesgo documentado	☐	☐	☐	☐

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 C-VT (Sección 2), con fecha *(fecha de finalización del SAQ).*

Según los resultados observados en el SAQ C-VT 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 C-VT 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[2], datos de CAV2, CVC2, CID, o CVV2[3], ni datos de PIN[4] 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:	

[2] 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.

[3] 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.

[4] 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	
1	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.	☐	☐	
2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.	☐	☐	
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.	☐	☐	
5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.	☐	☐	
6	Desarrollar y mantener sistemas y aplicaciones seguros	☐	☐	
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.	☐	☐	
8	Identificar y autenticar el acceso a los componentes del sistema.	☐	☐	
9	Restringir el acceso físico a los datos del titular de la tarjeta.	☐	☐	
11	Probar periódicamente los sistemas y procesos de seguridad.	☐	☐	
12	Mantener una política que aborde la seguridad de la información para todo el personal	☐	☐	
Anexo A2	Requisitos adicionales de las PCI DSS para las entidades que utilizan SSL/TLS temprana	☐	☐	

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