



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

**Comerciantes dedicados al comercio electrónico
parcialmente tercerizados que emplean un sitio
web externo para el procesamiento de pagos**

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
N/C	2.0		No utilizado
Febrero de 2014	3.0		El nuevo SAQ se ha desarrollado para abordar los requisitos que corresponden a los comerciantes dedicados al comercio electrónico con un sitio web que no reciben los datos del titular de la tarjeta, pero que afecta la seguridad de la transacción de pago y/o la integridad de la página que acepta los datos del titular de la tarjeta del consumidor. El contenido se alinea con los requisitos y procedimientos de prueba de las PCI DSS v3.0
Abril de 2015	3.1		Se actualizó para conseguir alineación con las PCI DSS v3.1. Para conocer en detalle los cambios de las PCI DSS, consulte <i>PCI DSS – Resumen de cambios de las PCI DSS versión 3.0 a 3.1</i> .
Junio de 2015	3.1		Actualizar requisito 11.3 para reparar el error.
Julio de 2015	3.1	1.1	Se actualizó para eliminar las referencias a las “mejores prácticas” antes del 30 de junio de 2015, y eliminar la opción de presentación de informes de PCI DSS v2 para el Requisito 11.3.
Abril de 2016	3.2	1.0	Se actualizó para conseguir alineación con las PCI DSS v3.2. Para conocer en detalle los cambios de las PCI DSS, consulte <i>PCI DSS – Resumen de cambios de las PCI DSS versión 3.1 a 3.2</i> . Requisitos añadidos de PCI DSS v3.2 Requisitos 1, 5, 6, 7, 8, 10, 11 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.

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

Modificaciones realizadas a los documentos	i
Antes de comenzar	v
Pasos para la realización de la autoevaluación de las PCI DSS	vi
Comprensión del cuestionario de autoevaluación	vi
<i>Pruebas esperadas</i>	<i>vi</i>
Respuestas del cuestionario de autoevaluación	vii
Guía para la no aplicabilidad de ciertos requisitos específicos	vii
Excepción legal	vii
Sección 1: Información sobre la evaluación	1
Sección 2: Cuestionario de autoevaluación A-EP.....	5
Desarrollar y mantener una red segura	5
<i>Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos</i>	<i>5</i>
<i>Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.....</i>	<i>9</i>
Proteger los datos del titular de la tarjeta.....	15
<i>Requisito 3: Proteger los datos almacenados del titular de la tarjeta.....</i>	<i>15</i>
<i>Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas</i>	<i>16</i>
Mantener un programa de administración de vulnerabilidad.....	18
<i>Requisito 5: Proteger todos los sistemas de malware y actualizar los programas o software antivirus regularmente</i>	<i>18</i>
<i>Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros</i>	<i>20</i>
Implementar medidas sólidas de control de acceso	27
<i>Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa</i>	<i>27</i>
<i>Requisito 8: Identifique y autentique el acceso a los componentes del sistema.....</i>	<i>28</i>
<i>Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.....</i>	<i>34</i>
Supervisar y evaluar las redes con regularidad	36
<i>Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta</i>	<i>36</i>
<i>Requisito 11: Probar periódicamente los sistemas y procesos de seguridad</i>	<i>42</i>
Mantener una política de seguridad de información	48
<i>Requisito 12: Mantener una política que aborde la seguridad de la información para todo el personal</i>	<i>48</i>
Anexo A: Requisitos adicionales de las PCI DSS	51
<i>Anexo A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido....</i>	<i>51</i>
<i>Anexo A2: Requisitos adicionales de las PCI DSS para las entidades que utilizan SSL/TLS temprana.....</i>	<i>51</i>

Anexo A3: Validación suplementaria de las entidades designadas (DESV) 52

Anexo B: Hoja de trabajo de controles de compensación 53

Anexo C: Explicaciones de no aplicabilidad 54

Sección 3: Detalles de la validación y la atestación 55

Antes de comenzar

El SAQ A-EP se ha desarrollado para abordar los requisitos que corresponden a los comerciantes dedicados al comercio electrónico con sitio web que no reciben los datos de los titulares de las tarjetas, pero que afectan la seguridad de la transacción de pago o la integridad de la página que acepta los datos de los titulares de las tarjetas del consumidor.

Los comerciantes correspondientes al SAQ A-EP son comerciantes dedicados al comercio electrónico que parcialmente tercerizan su canal de pago del mencionado comercio electrónico a terceros validados por las PCI DSS, y no almacenan, procesan ni transmiten en forma electrónica datos de los titulares de tarjetas en sus sistemas o locales.

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

- Su empresa maneja solamente transacciones de comercio electrónico;
- Todo el procesamiento de los datos de los titulares de las tarjetas se terceriza en su totalidad a procesadores de pagos externos validados por las PCI DSS;
- Su sitio web de comercio electrónico no recibe los datos de los titulares de las tarjetas pero controla de qué manera los consumidores, o sus datos de titulares de tarjeta, son redirigidos hacia un procesador de pago externo validado por las PCI DSS;
- Si el sitio web del comerciante está alojado por un proveedor externo, este proveedor está validado según todos los requisitos de las PCI DSS correspondientes (por ejemplo, incluido el Anexo A de las PCI DSS si el proveedor es un proveedor de hosting compartido);
- Todos los elementos presentes en las páginas de pago que se entregan al explorador del consumidor tienen su origen en el sitio web del comerciante o en los proveedores de servicios que cumplen con las PCI DSS;
- Su empresa no almacena, procesa ni transmite en forma electrónica datos de los titulares de tarjetas en sus sistemas o locales, sino que depende completamente de un uno o varios terceros que realizan estas funciones;
- Su empresa ha confirmado que el tercero o los terceros que manejan el almacenamiento, el procesamiento y/o la transmisión de los datos de los titulares de tarjetas cumplen con las PCI DSS; **y**
- Su empresa retiene solamente informes o recibos en papel con datos de los titulares de tarjetas, y estos documentos no se reciben por medios electrónicos.

Este SAQ se aplica solamente 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.

Nota: Para fines de este SAQ, los requisitos de PCI DSS que se refieren al “entorno de datos del titular de la tarjeta” son aplicables a la página(s) web del comerciante. Esto se debe a que el sitio web del comerciante afecta directamente a la forma en que se transmiten los datos de las tarjetas de pago, a pesar de que el propio sitio web no recibe los datos del titular de la tarjeta.

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 A-EP)
 - 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 adquirente, a la marca de pago o a otro solicitante.

Comprensión del cuestionario de autoevaluación

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

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

Documento	Incluye:
PCI DSS <i>(Requisitos de la norma de seguridad de datos de la PCI y procedimientos de evaluación de seguridad)</i>	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Información respecto de todos los SAQ y los criterios de elegibilidad que presentan • Método para determinar qué SAQ es el apropiado para su organización
<i>Glosario de términos, abreviaturas y acrónimos de las PCI DSS y PA-DSS</i>	<ul style="list-style-type: none"> • 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)	<p>La prueba esperada se ha realizado, y todos los requisitos se han cumplido con ayuda de un control de compensación.</p> <p>Todas las respuestas en esta columna requieren que se complete una Hoja de trabajo de controles de compensación (CCW) en el Anexo B del SAQ.</p> <p>La información respecto del uso de los controles de compensación y las pautas para completar la hoja de trabajo se proporcionan en las PCI DSS.</p>
No	Algunos de los elementos presentes en el requisito, o todos ellos, no se han cumplido, están en proceso de implementarse o es necesario realizar más pruebas antes de poder establecer si están implementados.
N/C (No corresponde)	<p>El requisito no se aplica al entorno de la organización. (Consulte la <i>Guía para la no aplicabilidad de ciertos requisitos específicos</i> que se ofrece debajo para conocer ejemplos).</p> <p>Todas las respuestas en esta columna requieren una explicación de respaldo en el Anexo C del SAQ.</p>

Guía para la no aplicabilidad de ciertos requisitos específicos

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

Excepción legal

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

Sección 1: Información sobre la evaluación

Instrucciones para la presentación

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

Parte 1. Información sobre Comerciante y Asesor de Seguridad Certificado

Parte 1a. Información de la organización del comerciante

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

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

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

Parte 2. Resumen ejecutivo

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

<input type="checkbox"/> Comercio minorista	<input type="checkbox"/> Telecomunicaciones	<input type="checkbox"/> Tiendas de comestibles y supermercados
<input type="checkbox"/> Petróleo	<input type="checkbox"/> Comercio electrónico	<input type="checkbox"/> Pedidos por correo/teléfono (MOTO)
<input type="checkbox"/> Otros (especifique):		

<p>¿Cuáles son los tipos de canales de pago a los que presta servicios su empresa?</p> <p><input type="checkbox"/> Pedidos por correo/teléfono (MOTO)</p> <p><input type="checkbox"/> Comercio electrónico</p> <p><input type="checkbox"/> Tarjeta presente (en persona)</p>	<p>¿Cuáles son los canales de pago que este SAQ abarca?</p> <p><input type="checkbox"/> Pedidos por correo/teléfono (MOTO)</p> <p><input type="checkbox"/> Comercio electrónico</p> <p><input type="checkbox"/> Tarjeta presente (en persona)</p>
--	---

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

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

Parte 2c. Ubicaciones

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

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

Parte 2d. Aplicación de pago

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

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

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

Parte 2e. Descripción del entorno

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

Por ejemplo:

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

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

Sí No

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

Parte 2f. Proveedores de servicio externos

¿Su empresa utiliza un Integrador o revendedor certificado (QIR)?

Sí No

En caso de ser Sí:

Nombre de la empresa QIR:

Nombre individual del QIR:

Descripción de los servicios proporcionados por QIR:

¿Su empresa comparte los datos de los titulares de tarjeta con uno o más proveedores de servicio externos (por ejemplo, Integrador o revendedor certificado (QIR), empresas de puertas de enlace, procesadores de pago, proveedores de servicio de pago (PSP), empresas de Web hosting, agentes de reservas en aerolíneas, agentes del programa de lealtad, etc.)?

Sí No

En caso de ser Sí:

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

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

Parte 2g. Elegibilidad para completar el SAQ A-EP

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

<input type="checkbox"/>	Los comerciantes solamente aceptan transacciones de comercio electrónico;
<input type="checkbox"/>	Todo el procesamiento de los datos de los titulares de las tarjetas se terceriza en su totalidad a procesadores de pagos externos validados por las PCI DSS;
<input type="checkbox"/>	El sitio web de comercio electrónico del comerciante no recibe los datos de los titulares de las tarjetas pero controla de qué manera los consumidores, o sus datos de titulares de tarjeta, son redirigidos hacia un procesador de pago externo validado por las PCI DSS;
<input type="checkbox"/>	Si el sitio web del comerciante está alojado por un proveedor externo, este proveedor está validado según todos los requisitos de las PCI DSS correspondientes (por ejemplo, incluido el Anexo A de las PCI DSS si el proveedor es un proveedor de hosting compartido);
<input type="checkbox"/>	Todos los elementos presentes en las páginas de pago que se entregan al explorador del consumidor tienen su origen en el sitio web del comerciante o en los proveedores de servicios que cumplen con las PCI DSS;
<input type="checkbox"/>	El comerciante no almacena, procesa ni transmite en forma electrónica datos de los titulares de tarjetas en sus sistemas o locales, sino que depende completamente de uno o varios terceros que realizan estas funciones;
<input type="checkbox"/>	El comerciante ha confirmado que el tercero o los terceros que manejan el almacenamiento, el procesamiento y/o la transmisión de los datos de los titulares de tarjetas cumplen con las PCI DSS; y
<input type="checkbox"/>	El comerciante retiene solamente informes o recibos en papel con datos de los titulares de tarjetas, y estos documentos no se reciben por medios electrónicos.

Sección 2: Cuestionario de autoevaluación A-EP

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:

Desarrollar y mantener una red segura

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
1.1	¿Están las normas de configuración del firewall y router establecidas e implementadas para incluir lo siguiente?					
1.1.1	¿Existe un proceso formal para aprobar y probar todos los cambios y las conexiones externas de red en las configuraciones de los firewalls y los routers?	<ul style="list-style-type: none"> Revisar el proceso documentado Entrevistar al personal Examinar las configuraciones de red 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(a) ¿Existe un diagrama de red actual que documenta todas las conexiones entre el entorno de los datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica?	<ul style="list-style-type: none"> Revisar el diagrama de red actual Examinar las configuraciones de red 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Hay un proceso implementado para asegurar que se mantiene actualizado el diagrama?	<ul style="list-style-type: none"> Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(a) ¿Existe un diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes?	<ul style="list-style-type: none"> Revisar el diagrama de flujo de datos actual Examinar las configuraciones de red 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Hay un proceso implementado para asegurar que se mantiene actualizado el diagrama?	<ul style="list-style-type: none"> Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	(a) ¿Es necesario tener un firewall implementado en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall Observar las configuraciones de red para verificar que hay un firewall implementado 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
	(b) ¿Se corresponde el diagrama actual de la red con las normas de configuración de firewalls?	<ul style="list-style-type: none"> Comparar las normas de configuración de firewall con el diagrama actual de red 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	(a) ¿Las normas de configuración del firewall y del router incluyen una lista documentada de servicios, protocolos y puertos, incluida la justificación y la aprobación comercial para cada una?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall y el router 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Son necesarios todos los servicios, protocolos y puertos no seguros, y se documentaron e implementaron características de seguridad para cada uno de ellos?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall y el router Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	(a) ¿Requieren las normas de configuración de firewalls y routers la revisión del conjunto de reglas de éstos, por lo menos, cada seis meses?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall y el router 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se revisan los conjuntos de reglas del firewall y router, por lo menos, cada seis meses?	<ul style="list-style-type: none"> Examinar la documentación de las revisiones del firewall 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2	<p>¿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?</p> <p>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.</p>					
1.2.1	(c) ¿Está restringido el tránsito entrante y saliente a la cantidad necesaria para el entorno de los datos de titulares de tarjetas?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall y el router Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) ¿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)?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall y el router Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
1.2.2	¿Están los archivos de configuración del router seguros y sin riesgo de acceso no autorizado y sincronizados, por ejemplo, la configuración en ejecución (o activa) coincide con la configuración de inicio (que se utiliza cuando se reinician las máquinas)?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall y el router Examinar los archivos de configuración de routers y las configuraciones de routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Revisar las normas de configuración del firewall y el router Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?					
1.3.1	¿Se implementó un DMZ para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado?	<ul style="list-style-type: none"> Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	¿Está restringido el tránsito entrante de Internet a las direcciones IP dentro del DMZ?	<ul style="list-style-type: none"> Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	¿Hay implementadas medidas antisuplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red? (Por ejemplo, bloquear el tráfico proveniente de Internet con una dirección interna).	<ul style="list-style-type: none"> Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	¿Está el tráfico saliente desde el entorno de datos del titular de la tarjeta a Internet expresamente autorizado?	<ul style="list-style-type: none"> Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	¿Solo se permite la entrada a la red de conexiones establecidas?	<ul style="list-style-type: none"> Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
1.3.7 (e) ¿Se implementaron métodos para prevenir la divulgación de direcciones IP privadas e información de enrutamiento desde en Internet? Nota: Entre los métodos para ocultar direcciones IP, se pueden incluir, a modo de ejemplo, los siguientes: <ul style="list-style-type: none"> • Traducción de Dirección de Red (NAT) • Ubicación de los servidores que contengan datos del titular de la tarjeta detrás de los servidores proxy/firewalls. • Eliminación o filtrado de anuncios de enrutamiento para redes privadas que emplean direcciones registradas, Uso interno del espacio de direcciones RFC1918 en lugar de direcciones registradas. 	<ul style="list-style-type: none"> ▪ Examinar las configuraciones de firewalls y routers 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(f) ¿Se autorizó la divulgación de direcciones IP privadas y de información de enrutamiento a entidades externas?	<ul style="list-style-type: none"> ▪ Examinar las configuraciones de firewalls y routers ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> ▪ Revisar las normas de configuración y las políticas ▪ Examinar los dispositivos móviles y/o propiedad de los empleados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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?	<ul style="list-style-type: none"> ▪ Revisar las normas de configuración y las políticas ▪ Examinar los dispositivos móviles y/o propiedad de los empleados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
1.5	<p>¿Las políticas de seguridad y los procedimientos operativos para la administración de firewalls</p> <ul style="list-style-type: none"> ▪ están documentados? ▪ están en uso? ▪ son de conocimiento para todas las partes afectadas? 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos operativos de seguridad ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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	<p>(g) ¿Se cambian siempre los valores predeterminados por el proveedor antes de instalar un sistema en la red?</p> <p><i>Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS (puntos de venta), las aplicaciones de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.</i></p>	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Examinar la documentación del proveedor ▪ Observar las configuraciones del sistema y las configuraciones de cuenta ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<p>(h) ¿Se eliminan o desactivan las cuentas predeterminadas que no son necesarias antes de instalar un sistema en la red?</p>	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema y las configuraciones de cuenta ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
2.2 (a) ¿Se desarrollaron normas de configuración para todos los componentes del sistema, las cuales, además, se corresponden con las normas de alta seguridad aceptadas en la industria? <i>Entre las fuentes de normas de alta seguridad aceptadas en la industria se pueden incluir, a modo de ejemplo, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) y Center for Internet Security (CIS).</i>	<ul style="list-style-type: none"> ▪ Revisar las normas de configuración del sistema ▪ Revisar las normas de alta seguridad aceptadas en la industria ▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se actualizan las normas de configuración del sistema cuando se identifican nuevos problemas de vulnerabilidad, tal como se define en el requisito 6.1?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Se aplican las normas de configuración de sistemas cuando se configuran nuevos sistemas?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
	(d) ¿Incluyen las normas de configuración de sistemas todo lo siguiente? <ul style="list-style-type: none"> • Cambiar los valores predeterminados de los proveedores y eliminar las cuentas predeterminadas innecesarias. • Implementar solo una función principal por servidor a fin de evitar que coexistan funciones que requieran diferentes niveles de seguridad en el mismo servidor. • Habilitar solo los servicios, protocolos, daemons, etc., necesarios, según lo requiera la función del sistema. • Implementar funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros. • Configurar los parámetros de seguridad del sistema para evitar el uso indebido. • Eliminar todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios. 	<ul style="list-style-type: none"> ▪ Revisar las normas de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	(i) ¿Se implementó una sola función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor? <i>Por ejemplo, los servidores web y DNS se deben implementar en servidores separados.</i>	<ul style="list-style-type: none"> ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Si se utilizan tecnologías de virtualización, se implementa una sola función principal por componente de sistema o dispositivo virtual?	<ul style="list-style-type: none"> ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
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)?	<ul style="list-style-type: none"> Revisar las normas de configuración Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(j) ¿Están todos los servicios, daemons o protocolos habilitados que no son seguros justificados de conformidad con las normas de configuración documentadas?	<ul style="list-style-type: none"> Revisar las normas de configuración Entrevistar al personal Examinar los parámetros de configuración Comparar los servicios habilitados, etc. con las justificaciones documentadas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	¿Están implementadas y documentadas las funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros? <i>Nota: Cuando se utiliza SSL/TLS temprana, deben completarse los requisitos establecidos en el Anexo A2.</i>	<ul style="list-style-type: none"> Revisar las normas de configuración Examinar los parámetros de configuración 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Están incluidos los parámetros de configuración de seguridad del sistema en las normas de configuración de sistemas?	<ul style="list-style-type: none"> Revisar las normas de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
	(c) ¿Se configuraron apropiadamente los parámetros de seguridad en los componentes del sistema?	<ul style="list-style-type: none"> ▪ Examinar los componentes del sistema ▪ Examinar la configuración de los parámetros de seguridad ▪ Comparar la configuración con las normas de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> ▪ Examinar los parámetros de seguridad en los componentes del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se documentaron todas las funciones habilitadas y admiten estas una configuración segura?	<ul style="list-style-type: none"> ▪ Revisar la documentación ▪ Examinar los parámetros de seguridad en los componentes del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Están presentes en los componentes del sistema solo las funcionalidades documentadas?	<ul style="list-style-type: none"> ▪ Revisar la documentación ▪ Examinar los parámetros de seguridad en los componentes del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.3	<p>¿Se cifró el acceso administrativo que no es de consola de la siguiente manera?</p> <p>Nota: Cuando se utiliza SSL/TLS temprana, deben completarse los requisitos establecidos en el Anexo A2.</p>					
	(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?	<ul style="list-style-type: none"> ▪ Examinar los componentes del sistema ▪ Examinar las configuraciones del sistema ▪ Observar a un administrador mientras se conecta 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
(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?	<ul style="list-style-type: none"> ▪ Examinar los componentes del sistema ▪ Examinar servicios y archivos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿El acceso de administradores a la interfaz de administración basada en la web está cifrado mediante una sólida criptografía?	<ul style="list-style-type: none"> ▪ Examinar los componentes del sistema ▪ Observar a un administrador mientras se conecta 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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?	<ul style="list-style-type: none"> ▪ Examinar los componentes del sistema ▪ Revisar la documentación del proveedor ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Examinar las configuraciones del sistema ▪ Examinar los procesos de eliminación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(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)?	<ul style="list-style-type: none"> ▪ Examinar fuentes de datos, incluidas las siguientes: <ul style="list-style-type: none"> • Datos de transacciones entrantes • Todos los registros • Archivos de historial • Archivos de seguimiento • Esquemas de bases de datos • Contenidos de bases de datos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	¿No se almacena el número de identificación personal (PIN) ni el bloqueo del PIN cifrado después de la autorización?	<ul style="list-style-type: none"> ▪ Examinar fuentes de datos, incluidas las siguientes: <ul style="list-style-type: none"> • Datos de transacciones entrantes • Todos los registros • Archivos de historial • Archivos de seguimiento • Esquemas de bases de datos • Contenidos de bases de datos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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? <i>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).</i>	<ul style="list-style-type: none"> ▪ 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Solo se aceptan claves/certificados de confianza?	<ul style="list-style-type: none"> ▪ Observar las transmisiones entrantes y salientes ▪ Examinar claves y certificados de confianza 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(k) ¿Hay implementados protocolos de seguridad para utilizar solo configuraciones seguras y no admitir versiones o configuraciones inseguras?	<ul style="list-style-type: none"> ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(l) ¿Se implementa el nivel de cifrado adecuado para la metodología de cifrado que se utiliza (ver recomendaciones de proveedores/mejores prácticas)?	<ul style="list-style-type: none"> ▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	
<p>(m) Para las implementaciones de TLS, ¿está TLS habilitado al transmitir o recibir los datos del titular de la tarjeta?</p> <p><i>Por ejemplo, para implementaciones basadas en explorador web:</i></p> <ul style="list-style-type: none"> • “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. 	<ul style="list-style-type: none"> ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4.2	<p>(b) ¿Se han puesto en práctica políticas que especifiquen que no se deben enviar números PAN sin protección a través de las tecnologías de mensajería del usuario final?</p>	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.3	<p>¿Las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de datos de titulares de tarjeta</p> <ul style="list-style-type: none"> ▪ están documentados? ▪ están en uso? ▪ son de conocimiento para todas las partes afectadas? 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos operativos de seguridad ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?	<ul style="list-style-type: none"> Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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)?	<ul style="list-style-type: none"> Revisar la documentación del proveedor Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	¿Todos los mecanismos de antivirus cumplen con lo siguiente?					
	(a) ¿Están actualizados el software antivirus y las definiciones?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos Examinar las configuraciones de antivirus, incluida la instalación maestra Examinar los componentes del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Están habilitados los análisis periódicos y las actualizaciones automáticas, y se los realiza?	<ul style="list-style-type: none"> Examinar las configuraciones de antivirus, incluida la instalación maestra Examinar los componentes del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
	(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?	<ul style="list-style-type: none"> Examinar las configuraciones de antivirus Revisar los procesos de retención de registros 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<p>¿Todos los mecanismos antivirus</p> <ul style="list-style-type: none"> están funcionando activamente? ¿Los mecanismos antivirus no pueden ser deshabilitados ni alterados por usuarios? <p><i>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.</i></p>	<ul style="list-style-type: none"> Examinar las configuraciones de antivirus Examinar los componentes del sistema Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.4	<p>¿Las políticas de seguridad y los procedimientos operativos para la protección contra malware</p> <ul style="list-style-type: none"> están documentados? están en uso? son de conocimiento para todas las partes afectadas? 	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos operativos de seguridad Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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
<p>6.1 ¿Existe un proceso para identificar vulnerabilidades de seguridad, incluida la siguiente?</p> <ul style="list-style-type: none"> ▪ ¿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”? <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
6.2	(n) ¿Están todos los programas de software y componentes del sistema protegidos de las vulnerabilidades conocidas mediante parches de seguridad instalados proporcionados por los proveedores?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(o) ¿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.	<ul style="list-style-type: none"> 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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.5	(a) ¿Se documentan los procedimientos de control de cambios y requieren lo siguiente? <ul style="list-style-type: none"> Documentación de incidencia Aprobación de control de cambio documentada por las partes autorizadas Pruebas de funcionalidad a fin de verificar que el cambio no impacta negativamente en la seguridad del sistema. Procedimientos de desinstalación 	<ul style="list-style-type: none"> Revisar los procesos y procedimientos de control de cambio 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se realiza y documenta lo siguiente para todos los cambios?					
6.4.5.1	¿Documentación de incidencia?	<ul style="list-style-type: none"> Realizar un seguimiento a la documentación del control de cambios Examinar la documentación del control de cambios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	
6.4.5.2	¿Aprobación de cambio documentada por las partes autorizadas?	<ul style="list-style-type: none"> Realizar un seguimiento a la documentación del control de cambios Examinar la documentación del control de cambios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.5.3	(a) Pruebas de funcionalidad a fin de verificar que el cambio no impacta negativamente en la seguridad del sistema.	<ul style="list-style-type: none"> Realizar un seguimiento a la documentación del control de cambios Examinar la documentación del control de cambios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿En el caso de cambios del código personalizado, se prueban las actualizaciones en cumplimiento con el Requisito 6.5 de las PCI DSS antes de la implementación para producción?	<ul style="list-style-type: none"> Realizar un seguimiento a la documentación del control de cambios Examinar la documentación del control de cambios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.5.4	¿Procedimientos de desinstalación?	<ul style="list-style-type: none"> Realizar un seguimiento a la documentación del control de cambios Examinar la documentación del control de cambios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.6	Al término de un cambio significativo, ¿se implementan todos los requisitos pertinentes de las PCI DSS en todos los sistemas y redes nuevos o modificados y se actualiza la documentación según corresponda? <i>Nota: Este requisito se considerará una mejor práctica hasta el 31 de enero de 2018, momento a partir del cual se convertirá en requisito.</i>	<ul style="list-style-type: none"> Realizar un seguimiento a la documentación del control de cambios Examinar la documentación del control de cambios Entrevistar al personal Observar los sistemas o redes afectados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5	¿Los procesos de desarrollo de software corrigen las vulnerabilidades de codificación comunes?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos del desarrollo de software 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
	¿Se capacita a los desarrolladores, por lo menos anualmente, en las técnicas actualizadas de codificación segura, incluido cómo evitar las vulnerabilidades comunes de codificación?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Examinar los registros de capacitación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Se desarrollan las aplicaciones en función de las pautas de codificación de seguridad para proteger las aplicaciones, al menos, contra las siguientes vulnerabilidades?					
6.5.1	<p>¿Las técnicas de codificación corrigen los errores de inyección, en especial errores de inyección SQL?</p> <p>Nota: También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.</p>	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.2	¿Las técnicas de codificación corrigen las vulnerabilidades creadas por el desbordamiento del buffer?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.4	¿Las técnicas de codificación corrigen las comunicaciones no seguras?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.5	¿Las técnicas de codificación corrigen el manejo inadecuado de errores?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.6	¿Las técnicas de codificación corrigen todas las vulnerabilidades “altas” detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.1 de las PCI DSS)?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	
En el caso de las aplicaciones web y las interfaces de las aplicaciones (internas o externas), existen aplicaciones desarrolladas en función de las pautas para la codificación segura para proteger las aplicaciones de las siguientes vulnerabilidades adicionales:				<input type="checkbox"/>	<input type="checkbox"/>	
6.5.7	¿Las técnicas de codificación corrigen las vulnerabilidades creadas por el lenguaje de comandos entre distintos sitios (XSS)?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.8	¿Las técnicas de codificación corrigen el control de acceso inapropiado, como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios, y la no restricción de acceso a las funciones por parte de los usuarios?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.9	¿Las técnicas de codificación corrigen la falsificación de solicitudes entre distintos sitios (CSRF)?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.10	¿Las técnicas de codificación corrigen la autenticación y administración de sesión interrumpidas?	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
<p>6.6 ¿En cuanto a las aplicaciones web públicas, se tratan las nuevas amenazas y vulnerabilidades de manera constante, y se las protege contra ataques conocidos aplicando <i>alguno</i> de los siguientes métodos?</p> <ul style="list-style-type: none"> ▪ Revisión de aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, de la siguiente manera: <ul style="list-style-type: none"> – Por lo menos, anualmente – Después de cualquier cambio – Por una organización que se especialice en seguridad de aplicaciones – Al menos, todas las vulnerabilidades del Requisito 6.5 se incluyan en la evaluación – Que se corrijan todas las vulnerabilidades – Que la aplicación se vuelva a analizar después de las correcciones <p>Nota: Esta evaluación no es la misma que el análisis de vulnerabilidades realizado en el Requisito 11.2.</p> <p>– O –</p> <ul style="list-style-type: none"> ▪ Instalar una solución técnica automatizada que detecta y previene los ataques basados en la web (por ejemplo, un firewall de aplicaciones web) como sigue: <ul style="list-style-type: none"> – Se encuentre delante de las aplicaciones web públicas para detectar y prevenir ataques web. – Funcione activamente y esté actualizada, según corresponda. – Genere registros de auditoría. – Esté configurada para bloquear ataques web o para generar una alerta que se investiga de inmediato. 	<ul style="list-style-type: none"> ▪ Revisar los procesos documentados ▪ Entrevistar al personal ▪ Examinar los registros de las evaluaciones de seguridad de la aplicación ▪ Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
6.7	¿Las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones <ul style="list-style-type: none"> ▪ están documentados? ▪ están en uso? ▪ son de conocimiento para todas las partes afectadas? 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos operativos de seguridad ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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? <ul style="list-style-type: none"> ▪ ¿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? 	<ul style="list-style-type: none"> ▪ Examinar la política de control de acceso escrita ▪ Entrevistar al personal ▪ Entrevistar a la administración ▪ Revisar las identificaciones de los usuarios con privilegios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.3	¿El acceso se asigna según la tarea, la clasificación y la función de cada persona?	<ul style="list-style-type: none"> ▪ Examinar la política de control de acceso escrita ▪ Entrevistar a la administración ▪ Revisar las identificaciones de los usuarios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	¿Se requiere la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios?	<ul style="list-style-type: none"> ▪ Revisar las identificaciones de los usuarios ▪ Comparar con las aprobaciones documentadas ▪ Comparar los privilegios asignados con las aprobaciones documentadas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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	¿Están definidos e implementados los procedimientos y las políticas para los controles administrativos de identificación de usuarios para los usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera?					
8.1.1	¿Se asigna a todos los usuarios una ID única antes de permitirles tener acceso a componentes del sistema o a los datos de titulares de tarjetas?	<ul style="list-style-type: none"> ▪ Revisar los procedimientos de contraseña ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.2	¿Se controlan la adición, eliminación y modificación de las ID de usuario, credenciales y otros objetos de identificación, tales como las ID de usuario que solo se implementan con autorización (incluidas las que tienen privilegios específicos)?	<ul style="list-style-type: none"> ▪ Revisar los procedimientos de contraseña ▪ Examinar las identificaciones de usuario con privilegios y generales y las autorizaciones asociadas ▪ Observar los parámetros del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	¿Se desactiva o elimina de manera inmediata el acceso de cualquier usuario cesante?	<ul style="list-style-type: none"> ▪ Revisar los procedimientos de contraseña ▪ Examinar las cuentas de usuarios cesantes ▪ Revisar las listas de acceso actuales ▪ Observar los dispositivos de autenticación física devueltos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.4	¿Se eliminan o desactivan las cuentas de usuario que hayan permanecido inactivas dentro de 90 días?	<ul style="list-style-type: none"> ▪ Revisar los procedimientos de contraseña ▪ Observar las cuentas de usuario 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.5	(a) ¿Las cuentas utilizadas por los proveedores para el acceso, el mantenimiento o el soporte de los componentes del sistema mediante el acceso remoto están habilitadas solo durante el tiempo necesario, y luego se las deshabilita cuando no están en uso?	<ul style="list-style-type: none"> ▪ Revisar los procedimientos de contraseña ▪ Entrevistar al personal ▪ Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
	(b) ¿Las cuentas de acceso remoto de los proveedores son supervisadas solo cuando están utilizándose?	<ul style="list-style-type: none"> Entrevistar al personal Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.6	(a) ¿Están limitados los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos?	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.7	Después que se ha bloqueado una contraseña de usuario, ¿se establece la duración del bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario?	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.8	¿Si una sesión estuvo inactiva durante más de 15 minutos, se vuelven a autenticar los usuarios (por ejemplo, al volver a escribir la contraseña) para que se active nuevamente la terminal o sesión?	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2	<p>¿Además de asignar una ID única, se emplean uno o más de los siguientes métodos para autenticar a todos los usuarios?</p> <ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Observar los procesos de autenticación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.1	(a) ¿La criptografía sólida se utiliza para dejar ilegibles todas las credenciales de autenticación (como contraseñas/frases de seguridad) durante la transmisión y el almacenamiento en todos los componentes del sistema?	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Revisar la documentación del proveedor Examinar los parámetros de configuración del sistema Observar los archivos de contraseña Observar las transmisiones de datos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
8.2.2	¿Se verifica la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablecimientos de contraseña, entrega de nuevos tokens o generación de nuevas claves?	<ul style="list-style-type: none"> Revisar los procedimientos de autenticación Observar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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? <ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Examinar los parámetros de configuración del sistema para verificar los parámetros de la contraseña 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.4	(a) ¿Se cambian las contraseñas/frases de seguridad de los usuarios por lo menos una vez cada 90 días?	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.5	(a) ¿Debe una persona enviar una contraseña/frase de usuario nueva que sea diferente de cualquiera de las últimas cuatro contraseñas/frases de usuario que utilizó?	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Realizar una muestra de componentes del sistema Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.6	¿Se configuran las contraseñas/frases en un valor único para cada usuario la primera vez y durante el restablecimiento, y debe cada usuario cambiar su contraseña de inmediato después del primer uso?	<ul style="list-style-type: none"> Revisar los procedimientos de contraseña Examinar los parámetros de configuración del sistema Observar al personal de seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
8.3	<p>Se asegura todo el acceso administrativo sin consola individual y todo el acceso remoto al CDE usando la autenticación de múltiples factores, como sigue:</p> <p>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.</p>					
8.3.1	<p>¿Se incorpora la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE para el personal con acceso administrativo?</p> <p>Nota: Este requisito se considerará una mejor práctica hasta el 31 de enero de 2018, momento a partir del cual se convertirá en requisito.</p>	<ul style="list-style-type: none"> Examinar las configuraciones del sistema Observar el inicio de sesión del administrador en CDE 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3.2	<p>¿Está incorporada la autenticación de múltiples factores para el acceso remoto a la red desde fuera de la red por parte del personal (incluso usuarios y administradores) y todas las partes externas involucradas (que incluye acceso del proveedor para soporte o mantenimiento)?</p>	<ul style="list-style-type: none"> Examinar las configuraciones del sistema Observar al personal conectarse de manera remota 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.4	<p>(a) ¿Se documentan y comunican los procedimientos y las políticas de autenticación a todos los usuarios?</p>	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Revisar el método de distribución Entrevistar al personal Entrevistar a los usuarios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
(b) ¿Los procedimientos y las políticas de autenticación incluyen lo siguiente? <ul style="list-style-type: none"> • Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. • Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. • Instrucciones para no seleccionar contraseñas utilizadas anteriormente. • Instrucciones que indican que los usuarios deben cambiar contraseñas si se sospecha que la contraseña corre riesgos. 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación proporcionada a los usuarios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.5 ¿Se prohíben las cuentas y contraseñas grupales, compartidas o genéricas u otros métodos de autenticación, de la siguiente manera? <ul style="list-style-type: none"> ▪ 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? 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Examinar las listas de identificaciones de usuario ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.6 Si se utilizan otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.), ¿el uso de estos mecanismos está asignado de la siguiente manera? <ul style="list-style-type: none"> ▪ Los mecanismos de autenticación se deben asignar a una sola cuenta y no compartirlos entre varias. ▪ Se deben implementar controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder. 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Examinar los parámetros de configuración del sistema y/o los controles físicos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
8.8	¿Las políticas de seguridad y los procedimientos operativos para la identificación y autenticación <ul style="list-style-type: none"> ▪ están documentados? ▪ están en uso? ▪ son de conocimiento para todas las partes afectadas? 	<ul style="list-style-type: none"> ▪ Examinar las políticas de seguridad y los procedimientos operativos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
9.1	¿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?	<ul style="list-style-type: none"> ▪ Observar los controles de acceso físicos ▪ Observar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5	¿Todos los medios de almacenamiento están físicamente asegurados (incluyendo, sin sentido limitativo, computadoras, medios extraíbles electrónicos, recibos en papel, informes de papel y faxes)? <i>A los efectos del Requisito 9, "medios" se refiere a todos los medios en papel y electrónicos que contienen datos de titulares de tarjetas.</i>	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos para el resguardo seguro de los medios ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6	(a) ¿Se lleva un control estricto sobre la distribución interna o externa de cualquier tipo de medios de almacenamiento?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos para la distribución de los medios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Incluyen los controles lo siguiente:					
9.6.1	¿Están clasificados los medios de manera que se pueda determinar la confidencialidad de los datos?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos para la clasificación de los medios ▪ Entrevistar al personal de seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	¿Los medios se envían por correo seguro u otro método de envío que se pueda rastrear con precisión?	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Examinar los registros de seguimiento de la distribución de medios y los documentos relacionados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	¿Se obtiene la aprobación de la administración antes de que se trasladen los medios (especialmente cuando se distribuyen a personas)?	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Examinar los registros de seguimiento de la distribución de medios y los documentos relacionados 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	¿Se lleva un control estricto sobre el almacenamiento y accesibilidad de los medios?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
9.8	(a) ¿Se destruyen los medios cuando ya no sean necesarios para la empresa o por motivos legales?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos para la destrucción periódica de medios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Se realiza la destrucción de la siguiente manera?:					
9.8.1	(a) ¿Se cortan en tiras, incineran o hacen pasta los materiales de copias en papel para que no se puedan reconstruir los datos de titulares de tarjetas?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos para la destrucción periódica de medios Entrevistar al personal Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se destruirán de forma segura los contenedores que almacenan los materiales con información para impedir acceso al contenido?	<ul style="list-style-type: none"> Examinar la seguridad de los contenedores de almacenamiento 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Supervisar y evaluar las redes con regularidad

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y 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
10.1	¿Las pistas de auditoría están habilitadas y activas para los componentes del sistema?	<ul style="list-style-type: none"> Observar los procesos Entrevistar al administrador del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	¿El acceso a los componentes del sistema está vinculado a usuarios específicos?	<ul style="list-style-type: none"> Observar los procesos Entrevistar al administrador del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2	¿Se implementan pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos?					
10.2.2	Todas las acciones realizadas por personas con privilegios de raíz o administrativos.	<ul style="list-style-type: none"> Entrevistar al personal Observar los registros de auditoría Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.3	Acceso a todas las pistas de auditoría.	<ul style="list-style-type: none"> Entrevistar al personal Observar los registros de auditoría Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.4	Intentos de acceso lógico no válidos.	<ul style="list-style-type: none"> Entrevistar al personal Observar los registros de auditoría Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.5	Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.	<ul style="list-style-type: none"> Entrevistar al personal Observar los registros de auditoría Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
10.2.6	¿Hay inicialización, detención o pausa de los registros de auditoría?	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los registros de auditoría ▪ Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.7	¿Creación y eliminación de objetos de nivel de sistema?	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los registros de auditoría ▪ Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3	¿Se registran las siguientes entradas de pistas de auditoría de todos los componentes del sistema para cada evento?					
10.3.1	Identificación de usuarios.	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los registros de auditoría ▪ Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.2	Tipo de evento.	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los registros de auditoría ▪ Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.3	Fecha y hora.	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los registros de auditoría ▪ Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.4	Indicación de éxito o fallo.	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los registros de auditoría ▪ Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
10.3.5	Origen del evento.	<ul style="list-style-type: none"> Entrevistar al personal Observar los registros de auditoría Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.6	Identidad o nombre de los datos, componentes del sistema o recurso afectados.	<ul style="list-style-type: none"> Entrevistar al personal Observar los registros de auditoría Examinar los parámetros del registro de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4	<p>¿Se sincronizan todos los relojes y horas críticos del sistema a través del uso de la tecnología de sincronización de hora, la cual se mantiene actualizada?</p> <p>Nota: Un ejemplo de tecnología de sincronización es el NTP (protocolo de tiempo de red).</p>	<ul style="list-style-type: none"> Revisar las normas de configuración de hora y los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4.1	¿Están implementados los siguientes procesos para que los sistemas críticos tengan la hora correcta y correspondiente?					
(a)	¿Solamente los servidores de horario central designados reciben señales de tiempo de fuentes externas, y las señales de tiempo de fuentes externas están basadas en la hora atómica internacional o UTC?	<ul style="list-style-type: none"> Revisar las normas de configuración de hora y los procesos Examinar los parámetros del sistema relacionados con la hora 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b)	En los casos en los que hay más de un servidor de horario designado, ¿estos se emparejan para mantener la hora exacta?	<ul style="list-style-type: none"> Revisar las normas de configuración de hora y los procesos Examinar los parámetros del sistema relacionados con la hora 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c)	¿Los sistemas reciben información horaria solo de los servidores de horario central designados?	<ul style="list-style-type: none"> Revisar las normas de configuración de hora y los procesos Examinar los parámetros del sistema relacionados con la hora 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	
10.4.2	<p>¿Se protegen los datos de tiempo de la siguiente manera:</p> <p>(a) ¿Se restringe el acceso a los datos de tiempo solo a personal con una necesidad de negocio de acceder a dichos datos?</p> <p>(b) ¿Se registran, supervisan y revisan los cambios a los parámetros de hora en los sistemas críticos?</p>	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y los parámetros de sincronización de tiempo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4.3	<p>¿Se recibe la configuración de hora de fuentes específicas y aceptadas por la industria? (Esto es para impedir que una persona malintencionada cambie el reloj).</p> <p><i>De forma opcional, estas actualizaciones pueden cifrarse con una clave simétrica, y pueden crearse listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de hora (para evitar el uso no autorizado de servidores horarios internos).</i></p>	<ul style="list-style-type: none"> Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5	¿Se aseguran de la siguiente manera las pistas de auditoría de manera que no se puedan alterar?					
10.5.1	¿Se limita la visualización de pistas de auditoría a quienes lo necesitan por motivos de trabajo?	<ul style="list-style-type: none"> Entrevistar a los administradores del sistema Examinar las configuraciones y los permisos del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5.2	¿Están protegidos los archivos de las pistas de auditoría contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física y/o segregación de redes?	<ul style="list-style-type: none"> Entrevistar a los administradores del sistema Examinar las configuraciones y los permisos del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5.3	¿Se realizan de inmediato copias de seguridad de los archivos de las pistas de auditoría en un servidor de registros central o medios que resulten difíciles de modificar?	<ul style="list-style-type: none"> Entrevistar a los administradores del sistema Examinar las configuraciones y los permisos del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
10.5.4	¿Se copian los registros para tecnologías externas (por ejemplo, tecnologías inalámbricas, firewalls, DNS, correo) en medios o servidores de registros centralizados, internos y seguros?	<ul style="list-style-type: none"> ▪ Entrevistar a los administradores del sistema ▪ Examinar las configuraciones y los permisos del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5.5	¿Se utiliza el software de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta)?	<ul style="list-style-type: none"> ▪ Examinar los parámetros, los archivos monitorizados y los resultados de las actividades de supervisión 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6	<p>¿Se revisan los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas?</p> <p>Nota: Las herramientas de recolección, análisis y alerta de registros pueden ser utilizadas para lograr el cumplimiento con el Requisito 10.6</p>					
10.6.1	<p>(b) ¿Se revisan los siguientes eventos de seguridad y registros como mínimo diariamente, ya sea en forma manual o mediante herramientas de registro?</p> <ul style="list-style-type: none"> • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.). 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de seguridad ▪ Observar los procesos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
10.6.2	(b) ¿Se revisan periódicamente los registros de todos los demás componentes del sistema, ya sea de forma manual o con herramientas de registros, según la política y estrategia de gestión de riesgos de la organización?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de seguridad ▪ Revisar la documentación de evaluación de riesgo ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.3	(b) ¿Se identifica un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de seguridad ▪ Observar los procesos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7	(b) ¿Se retienen los registros de auditoría por al menos un año?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de seguridad ▪ Entrevistar al personal ▪ Examinar los registros de auditoría 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Se encuentran disponibles al menos los registros de los últimos tres meses para el análisis?	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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
11.2.2 (a) ¿Se realizan escaneos externos trimestrales de vulnerabilidades? <i>Nota: Los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor aprobado de análisis (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC). Consulte la Guía del programa de ASV (proveedor aprobado de escaneo) publicada en el sitio web del PCI SSC para obtener información sobre las responsabilidades de análisis del cliente, sobre la preparación del análisis, etc.</i>	<ul style="list-style-type: none"> Revisar los resultados de los escaneos de vulnerabilidades externos de los cuatro trimestres más recientes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Los resultados de cada escaneo y repetición de escaneo trimestral satisfacen los requisitos de la <i>Guía del programa ASV para la aprobación de los escaneos</i> ? (por ejemplo, ausencia de vulnerabilidades con calificación mayor que 4.0 por la CVSS y ausencia de fallas automáticas).	<ul style="list-style-type: none"> Revisar los resultados de cada escaneo y repetición de escaneo externo trimestral 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Los escaneos trimestrales de vulnerabilidades externas son realizados por Proveedores aprobados de escaneos (ASV), aprobados por PCI SSC?	<ul style="list-style-type: none"> Revisar los resultados de cada escaneo y repetición de escaneo externo trimestral 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.3 (a) ¿Se llevan a cabo análisis internos y externos, y se los repite, según sea necesario, después de realizar un cambio significativo? <i>Nota: Los análisis deben estar a cargo de personal calificado.</i>	<ul style="list-style-type: none"> Examinar y correlacionar la documentación de control de cambio y los informes de escaneo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
		Sí	Sí con CCW	No	N/C
(b) ¿El proceso de escaneo incluye nuevos análisis hasta que ocurre lo siguiente? <ul style="list-style-type: none"> No se han registrado vulnerabilidades con puntuaciones CSVV de 4.0 o superior en análisis externos. En escaneos internos, se ha obtenido un resultado de aprobación o se han resuelto todas las vulnerabilidades “Alta”, como las define el Requisito 6.1 de las PCI DSS. 	<ul style="list-style-type: none"> Revisar los informes de escaneo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Los escaneos son realizados por recurso(s) internos calificados o por terceros calificados y, si corresponde, la empresa que realiza las pruebas garantiza la independencia? (no es necesario que sea un QSA o ASV).	<ul style="list-style-type: none"> Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
11.3	<p>¿En la metodología de pruebas de penetración se incluye lo siguiente?</p> <ul style="list-style-type: none"> ▪ Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800-115). ▪ Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. ▪ Incluya pruebas del entorno interno y externo de la red. ▪ Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. ▪ Defina las pruebas de penetración de la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5. ▪ Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos. ▪ Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. ▪ Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección. 	<ul style="list-style-type: none"> ▪ Examinar la metodología de pruebas de penetración ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3.1	(a) ¿Se realizan <i>pruebas de penetración externas</i> según la metodología definida al menos una vez al año y después de cualquier modificación significativa de infraestructuras o aplicaciones en el entorno (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor web)?	<ul style="list-style-type: none"> ▪ Examinar el alcance del trabajo ▪ Examinar los resultados obtenidos de la última prueba de penetración externa 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿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).	<ul style="list-style-type: none"> ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
11.3.3	¿Las vulnerabilidades de seguridad detectadas en las pruebas de penetración se corrigen, y las pruebas se repiten para verificar las correcciones?	<ul style="list-style-type: none"> Examinar los resultados de las pruebas de penetración 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Examinar los controles de segmentación Revisar la metodología de pruebas de penetración 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b)	¿Las pruebas de penetración para verificar los controles de segmentación cumplen con lo siguiente? <ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Examinar los resultados de la prueba de penetración más reciente 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(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).	<ul style="list-style-type: none"> Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	
11.4	(a) ¿Hay implementadas técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red para supervisar todo el tráfico? <ul style="list-style-type: none"> En el perímetro del entorno de datos del titular de la tarjeta, y En los puntos críticos del entorno de datos del titular de la tarjeta. 	<ul style="list-style-type: none"> Examinar las configuraciones del sistema Examinar los diagramas de la red 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Las técnicas de intrusión-detección y de intrusión-prevención están configuradas para alertar al personal de posibles riesgos?	<ul style="list-style-type: none"> Examinar las configuraciones del sistema Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Se han actualizados todos los motores de detección y prevención de intrusiones, bases y firmas?	<ul style="list-style-type: none"> Examinar las configuraciones IDS/IPS Examinar la documentación del proveedor 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5	(a) ¿Se implementa un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de la integridad del archivo) para detectar la modificación no autorizada (incluidos los cambios, las adiciones y las eliminaciones) de los archivos críticos del sistema, los archivos de configuración o de contenido? <i>Los ejemplos de archivos que se deben supervisar incluyen:</i> <ul style="list-style-type: none"> Ejecutables del sistema Ejecutables de aplicaciones Archivos de configuración y parámetros Archivos de almacenamiento central, históricos o archivados, de registro y auditoría Archivos críticos adicionales que determine la entidad (por ejemplo, a través de la evaluación de riesgos u otros medios) 	<ul style="list-style-type: none"> Observar la configuración del sistema y los archivos monitoreados Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
	<p>(b) ¿Están configuradas las herramientas para alertar al personal ante modificaciones no autorizadas (incluidos los cambios, las adiciones y las eliminaciones) de archivos críticos del sistema, archivos de configuración o archivos de contenido, y dichas herramientas realizan comparaciones de archivos críticos al menos semanalmente?</p> <p>Nota: A los fines de la detección de cambios, generalmente, los archivos críticos son aquellos que no se modifican con regularidad, pero cuya modificación podría implicar un riesgo o peligro para el sistema. Generalmente, los mecanismos de detección de cambios, como los productos de supervisión de integridad de archivos, vienen preconfigurados con archivos críticos para el sistema operativo relacionado. La entidad (es decir el comerciante o el proveedor de servicios) debe evaluar y definir otros archivos críticos, tales como los archivos para aplicaciones personalizadas.</p>	<ul style="list-style-type: none"> Observar la configuración del sistema y los archivos monitoreados Revisar los resultados obtenidos de las actividades de supervisión 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5.1	¿Hay implementado un proceso para responder a las alertas que genera la solución de detección de cambios?	<ul style="list-style-type: none"> Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Mantener una política de seguridad de información

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

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

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
12.1	¿Existe una política de seguridad establecida, publicada, mantenida y divulgada al todo el personal pertinente?	<ul style="list-style-type: none"> Revisar la política de seguridad de información 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Revisar la política de seguridad de información Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.4	¿Las políticas y los procedimientos de seguridad definen claramente las responsabilidades de seguridad de la información de todo el personal?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos de seguridad de información Entrevistar a una muestra del personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos de seguridad de información 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> Revisar el programa de concienciación sobre seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)			
			Sí	Sí con CCW	No	N/C
12.8	¿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?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Observar los procesos ▪ Revisar la lista de proveedores de servicios. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.2	<p>¿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?</p> <p>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.</p>	<ul style="list-style-type: none"> ▪ Observar los acuerdos escritos ▪ Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	¿Existe un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso?	<ul style="list-style-type: none"> ▪ Observar los procesos ▪ Revisar las políticas y los procedimientos así como la documentación complementaria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	¿Se mantiene un programa para supervisar el estado de cumplimiento con las PCI DSS del proveedor de servicios con una frecuencia anual, como mínimo?	<ul style="list-style-type: none"> ▪ Observar los procesos ▪ Revisar las políticas y los procedimientos así como la documentación complementaria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	
12.8.5	¿Se conserva la información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad?	<ul style="list-style-type: none"> ▪ Observar los procesos ▪ Revisar las políticas y los procedimientos así como la documentación complementaria 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.1	(a) ¿Se ha creado un plan de respuesta a incidentes para implementarlo en caso de fallos en el sistema?	<ul style="list-style-type: none"> ▪ Revisar el plan de respuesta a incidentes ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Aborda el plan, como mínimo, lo siguiente?					
	<ul style="list-style-type: none"> • ¿Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago? 	<ul style="list-style-type: none"> ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • ¿Procedimientos específicos de respuesta a incidentes? 	<ul style="list-style-type: none"> ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • ¿Procedimientos de recuperación y continuidad comercial? 	<ul style="list-style-type: none"> ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • ¿Procesos de copia de seguridad de datos? 	<ul style="list-style-type: none"> ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • ¿Análisis de los requisitos legales para el informe de riesgos? 	<ul style="list-style-type: none"> ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> • ¿Cobertura y respuestas de todos los componentes críticos del sistema? 	<ul style="list-style-type: none"> ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> • ¿Referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago? 	<ul style="list-style-type: none"> ▪ Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Anexo A: Requisitos adicionales de las PCI DSS

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

Este anexo no se utiliza durante las evaluaciones de comerciantes.

Anexo A2: Requisitos 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	<p>Para los terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) utilizando SSL y/o TLS temprana:</p> <ul style="list-style-type: none"> Se confirmaron los dispositivos para que no sean susceptibles a ninguna explotación conocida para SSL/TLS temprana <p>O bien:</p> <ul style="list-style-type: none"> ¿Hay un Plan de migración y de Mitigación de riesgo formal implementado según el Requisito A2.2? 	<ul style="list-style-type: none"> 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. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	
A2.2	<p>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:</p> <ul style="list-style-type: none"> ▪ 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? 	<ul style="list-style-type: none"> ▪ Revisar el Plan de migración y de Mitigación de riesgo documentado 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

Anexo B: Hoja de trabajo de controles de compensación

Utilice esta hoja de trabajo para definir los controles de compensación para cualquier requisito en el que se marcó “Sí con CCW”.

Nota: Sólo las empresas que han llevado a cabo un análisis de riesgos y que tienen limitaciones legítimas tecnológicas o documentadas pueden considerar el uso de controles de compensación para lograr el cumplimiento.

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

Definición y número de requisito:

	Información requerida	Explicación
1. Limitaciones	Enumere las limitaciones que impiden el cumplimiento con el requisito original.	
2. Objetivo	Defina el objetivo del control original; identifique el objetivo con el que cumple el control de compensación.	
3. Riesgo identificado	Identifique cualquier riesgo adicional que imponga la falta del control original.	
4. Definición de controles de compensación	Defina controles de compensación y explique de qué manera identifican los objetivos del control original y el riesgo elevado, si es que existe alguno.	
5. Validación de controles de compensación	Defina de qué forma se validaron y se probaron los controles de compensación.	
6. Mantenimiento	Defina los procesos y controles que se aplican para mantener los controles de compensación.	

Sección 3: Detalles de la validación y la atestación

Parte 3. Validación de la PCI DSS

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

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

<input type="checkbox"/>	<p>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 (<i>nombre de la empresa del comerciante</i>) ha demostrado un cumplimiento total con la PCI DSS.</p>						
<input type="checkbox"/>	<p>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 (<i>nombre de la empresa del comerciante</i>) no ha demostrado un cumplimiento total con la PCI DSS.</p> <p>Fecha objetivo para el cumplimiento:</p> <p>Es posible que se exija a una entidad que presente este formulario con un estado de Falta de cumplimiento que complete el Plan de acción en la Parte 4 de este documento. <i>Consulte con su adquirente o la(s) marca(s) de pago antes de completar la Parte 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>Si está marcado, complete lo siguiente:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 35%;">Requisito afectado</th> <th>Detalles respecto de cómo la limitación legal impide que se cumpla el requisito</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> </tbody> </table>	Requisito afectado	Detalles respecto de cómo la limitación legal impide que se cumpla el requisito				
Requisito afectado	Detalles respecto de cómo la limitación legal impide que se cumpla el requisito						

Parte 3a. Reconocimiento de estado

Los firmantes confirman:

(**marque todo lo que corresponda**)

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

Parte 3a. Reconocimiento de estado(cont.)

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

Parte 3b. Declaración del comerciante

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

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

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

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

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

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

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

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

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

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

Seleccione la respuesta apropiada para “En cumplimiento con los requisitos de las PCI DSS” correspondiente para cada requisito. Si la respuesta a cualquier requisito es “No”, debe proporcionar la fecha en la que la empresa espera cumplir con el requisito y una breve descripción de las medidas que se tomarán para cumplirlo.

Consulte con su adquiriente o la(s) marca(s) de pago antes de completar la Parte 4.

Requisito de las PCI DSS*	Descripción del requisito	En cumplimiento con los requisitos de las PCI DSS (seleccione uno)		Fecha y medidas de corrección (si se seleccionó “NO” para algún requisito)
		SÍ	NO	
1	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.	<input type="checkbox"/>	<input type="checkbox"/>	
2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteja los datos del titular de la tarjeta que fueron almacenados	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.	<input type="checkbox"/>	<input type="checkbox"/>	
6	Desarrollar y mantener sistemas y aplicaciones seguros	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identificar y autenticar el acceso a los componentes del sistema.	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restringir el acceso físico a los datos del titular de la tarjeta.	<input type="checkbox"/>	<input type="checkbox"/>	
10	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Probar periódicamente los sistemas y procesos de seguridad.	<input type="checkbox"/>	<input type="checkbox"/>	
12	Mantener una política que aborde la seguridad de la información para todo el personal	<input type="checkbox"/>	<input type="checkbox"/>	
Anexo A2	Requisitos adicionales de las PCI DSS para las entidades que utilizan SSL/TLS temprana	<input type="checkbox"/>	<input type="checkbox"/>	

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

