



**Industria de Tarjetas de Pago (PCI)
Norma de seguridad de datos
Cuestionario de autoevaluación D
y Atestación de cumplimiento para
Proveedores de servicios**

Proveedores de servicio elegibles para el SAQ

Para su uso con la Versión 3.2 de las PCI DSS

Abril de 2016

Modificaciones realizadas a los documentos

Fecha	Versión de las PCI DSS	Revisión del SAQ	Descripción
Octubre de 2008	1.2		Alinear el contenido con la nueva versión 1.2 de PCI DSS e implementar cambios menores notados desde la versión 1.1 original.
Octubre de 2010	2.0		Para alinear el contenido con los requisitos y procedimientos de prueba de PCI DSS v2.0
Febrero de 2014	3.0		Para alinear el contenido con los requisitos y procedimientos de prueba de PCI DSS v3.0 e incorporar opciones de respuesta adicionales.
Abril de 2015	3.1		Se actualizó para conseguir alineación con las PCI DSS v3.1. Para conocer en detalle los cambios de las PCI DSS, consulte <i>PCI DSS – Resumen de cambios de las PCI DSS versión 3.0 a 3.1</i> .
Julio de 2015	3.1	1.1	Se actualizó 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> .

Índice

Modificaciones realizadas a los documentos	ii
Antes de comenzar	v
Pasos para la realización de la autoevaluación de las PCI DSS	v
Comprensión del cuestionario de autoevaluación	v
<i>Pruebas esperadas</i>	<i>vi</i>
Respuestas del cuestionario de autoevaluación	vi
Guía para la no aplicabilidad de ciertos requisitos específicos.....	vii
<i>Comprensión de la diferencia entre No corresponde y No probado</i>	<i>vii</i>
Excepción legal	viii
Sección 1: Información sobre la evaluación	1
Sección 2: Cuestionario de autoevaluación D paraproveedores de servicios	7
Desarrolle y mantenga redes y sistemas seguros.....	7
<i>Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos</i>	<i>7</i>
<i>Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores</i>	<i>13</i>
Proteger los datos del titular de la tarjeta.....	21
<i>Requisito 3: Proteger los datos almacenados del titular de la tarjeta.....</i>	<i>21</i>
<i>Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas</i>	<i>31</i>
Mantener un programa de administración de vulnerabilidad.....	33
<i>Requisito 5: Proteger todos los sistemas de malware y actualizar los programas o software antivirus regularmente</i>	<i>33</i>
<i>Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguros.....</i>	<i>35</i>
Implementar medidas sólidas de control de acceso	46
<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>46</i>
<i>Requisito 8: Identifique y autentique el acceso a los componentes del sistema.....</i>	<i>49</i>
<i>Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.....</i>	<i>58</i>
Supervisar y evaluar las redes con regularidad.....	67
<i>Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.....</i>	<i>67</i>
<i>Requisito 11: Probar periódicamente los sistemas y procesos de seguridad</i>	<i>77</i>
Mantener una política de seguridad de información	86
<i>Requisito 12: Mantener una política que aborde la seguridad de la información para todo el personal</i>	<i>86</i>
Anexo A: Requisitos adicionales de las PCI DSS	95
<i>Anexo A1: Requisitos adicionales de las PCI DSS para proveedores de hosting compartido..</i>	<i>95</i>
<i>Anexo A2: Requisitos adicionales de las PCI DSS para las entidades que utilizan SSL/TLS temprana.....</i>	<i>97</i>
<i>Anexo A3: Validación suplementaria de las entidades designadas (DESV).....</i>	<i>99</i>
Anexo B: Hoja de trabajo de controles de compensación	100

Anexo C: Explicaciones de no aplicabilidad..... 101
Anexo D: Explicación de los requisitos No probados 102
Sección 3: Detalles de la validación y la atestación103

Antes de comenzar

El SAQ D para proveedores de servicios se aplica a todos los proveedores de servicios definidos por una marca de pago como elegibles para el SAQ.

Si bien muchas de las organizaciones que completan el SAQ D deberán validar su cumplimiento con todos los requisitos de las PCI DSS, es posible que algunas de las organizaciones con modelos de negocio muy específicos encuentren que algunos requisitos no son aplicables. Consulte la directriz de abajo para obtener información sobre la exclusión de determinados requisitos específicos.

Pasos para la realización de la autoevaluación de las PCI DSS

1. Confirmar que su entorno cuenta con la delimitación del alcance apropiada.
2. Evalúe su entorno respecto del cumplimiento con los requisitos de las PCI DSS.
3. 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 D)
 - 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)
4. Presente el SAQ y la Atestación de cumplimiento (AOC), junto con cualquier otro documento solicitado, como los informes de análisis de ASV 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 en 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
<i>Documentos con instrucciones y pautas de SAQ</i>	<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 complementaria en el Anexo C del SAQ.</p>
No probado	<p>No estaba incluido el requisito para su consideración en la evaluación, y es por eso que no se lo evaluó de ninguna forma. (Consultar <i>Comprensión de la diferencia entre No corresponde y No probado</i> debajo para ver ejemplos de las ocasiones en las que debe utilizarse esta opción).</p> <p>Todas las respuestas en esta columna requieren una explicación complementaria en el Apéndice D del SAQ.</p>

Guía para la no aplicabilidad de ciertos requisitos específicos

Si bien muchas de las organizaciones que completan el SAQ D deberán validar su cumplimiento con todos los requisitos de las PCI DSS, es posible que algunas de las organizaciones con modelos de negocio muy específicos encuentren que algunos requisitos no son aplicables. Por ejemplo, no se esperaría de una compañía que no utiliza tecnología inalámbrica en modo alguno que valide el cumplimiento con las secciones de las PCI DSS relacionadas con el manejo de tecnología inalámbrica. De manera semejante, una organización que nunca almacena datos de titulares de tarjetas de manera electrónica no necesitará validar los requisitos que están relacionados con el almacenamiento seguro de los datos de los titulares de tarjetas (por ejemplo, el Requisito 3.4).

Entre los ejemplos de requisitos con aplicabilidad específica se incluyen:

- Las preguntas específicas relacionadas con las tecnologías inalámbricas seguras solo se deben responder si la tecnología inalámbrica está presente en cualquier parte de su red (por ejemplo, Requisitos 1.2.3, 2.1.1 y 4.1.1). Tenga en cuenta que el Requisito 11.1 (uso de procesos para la identificación de puntos de acceso inalámbrico no autorizados) se debe responder incluso si su red no utiliza tecnología inalámbrica, debido a que el proceso detecta cualesquiera dispositivos peligrosos no autorizados que se hayan podido agregar sin su consentimiento.
- Las preguntas específicas respecto del desarrollo de las aplicaciones y el código seguro (Requisitos 6.3 y 6.5) solo se deben responder si su organización desarrolla sus propias aplicaciones personalizadas.
- Las preguntas del Requisito 9.1.1 y 9.3 solo se deben responder si las instalaciones poseen “áreas confidenciales”, tal como se define aquí. “Áreas confidenciales” hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan procesos o transmitan datos de titulares de tarjetas. Esto excluye las áreas donde solo hay terminales de punto de venta, tales como el área de cajas de un comercio; no obstante, sí incluye las salas de servidores trastienda que almacenan datos de titulares de tarjetas y las áreas de almacenamiento de grandes cantidades de datos de titulares de tarjetas.

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”.

Comprensión de la diferencia entre No corresponde y No probado

Los requisitos que no se consideran aplicables a un entorno deberán verificarse como tales. Con el ejemplo de tecnología inalámbrica indicado anteriormente, para que una organización seleccione “N/C” para los Requisitos 1.2.3, 2.1.1, y 4.1.1, primero la organización debe confirmar que no se utilizan tecnologías inalámbricas en su CDE o que estén conectadas con su CDE. Una vez que esto se ha confirmado, la organización puede seleccionar “N/C” para esos requisitos específicos.

Si se excluye totalmente un requisito de la revisión sin consideración alguna respecto de si *podría* corresponder, se debe seleccionar la opción “No probado”. Algunos ejemplos de situaciones en las que podría ocurrir esto incluyen:

- Un adquiriente puede pedirle a una organización que valide un subconjunto de requisitos, por ejemplo: uso del enfoque priorizado para la validación de determinados logros.
- Es posible que una organización desee validar un nuevo control de seguridad cuyo impacto alcanza solamente a un subconjunto de requisitos, por ejemplo, la implementación de una nueva metodología de cifrado que requiere la evaluación de los Requisitos 2, 3 y 4 de las PCI DSS.
- Una organización de proveedor de servicio puede ofrecer un servicio que abarca únicamente una cantidad limitada de requisitos de las PCI DSS; por ejemplo, un proveedor de almacenamiento físico quizá desea validar solamente los controles de seguridad físicos según el Requisito 9 de las PCI DSS para su instalación de almacenamiento.

En estas situaciones, la organización solo desea la validación de determinados requisitos de las PCI DSS, incluso si hay otros requisitos que podrían corresponder a su entorno.

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 proveedor de servicios 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 proveedor de servicios es responsable de asegurarse que las partes relevantes completen cada sección según corresponda: Comuníquese con la marca de pago solicitante para establecer los procedimientos para la presentación y elaboración del informe.

Parte 1. Información sobre el proveedor de servicios y el asesor de seguridad calificado

Parte 1a. Información sobre la organización del proveedor de servicios

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. Verificación del alcance

Servicios que SE INCLUYERON en el alcance de la evaluación de las PCI DSS (marque todas las opciones aplicables)

Nombre de los servicios evaluados:

Tipo de los servicios evaluados:

Proveedor de hosting:

- Aplicación/software
- Hardware
- Infraestructura/red
- Espacio físico (cubicación)
- Almacenamiento
- Web
- Servicios de seguridad
- Proveedor de hosting 3-D Secure
- Proveedor de hosting compartido
- Otros hostings (especifique):

Servicios administrados (especificar):

- Servicios de seguridad de sistemas
- Soporte de TI
- Seguridad física
- Sistema de administración de terminales
- Otros servicios (especificar):

Procesamiento de pago:

- POS/tarjeta presente
- Internet/comercio electrónico
- MOTO/Centro de llamadas
- ATM
- Otro procesamiento (especifique):

Administración de cuentas

Fraude y reintegro de cobros

Conmutador/Puerta de enlace de pagos

Servicios administrativos

Procesamiento del emisor

Servicios prepagados

Administración de facturación

Programas de lealtad

Administración de registros

Compensación y liquidación

Servicios de comerciantes

Pagos de impuestos/gubernamentales

Proveedor de red

Otros (especifique):

Nota: Estas categorías se proporcionan únicamente a los fines de asistencia, y no tienen como finalidad limitar ni predeterminar la descripción de servicio de una entidad. Si considera que estas categorías no corresponden a su servicio, complete "Otras". Si tiene dudas respecto de la aplicabilidad de una categoría a su servicio, consulte con la marca de pago correspondiente.

Parte 2a. Verificación de alcance (continuación)

Servicios proporcionados por el proveedor de servicios pero que NO SE INCLUYERON en el alcance de la evaluación de las PCI DSS (marque todos los que correspondan)

Nombre de los servicios no evaluados:

Tipo de los servicios no evaluados:

Proveedor de hosting: <input type="checkbox"/> Aplicación/software <input type="checkbox"/> Hardware <input type="checkbox"/> Infraestructura/red <input type="checkbox"/> Espacio físico (cubicación) <input type="checkbox"/> Almacenamiento <input type="checkbox"/> Web <input type="checkbox"/> Servicios de seguridad <input type="checkbox"/> Proveedor de hosting 3-D Secure <input type="checkbox"/> Proveedor de hosting compartido <input type="checkbox"/> Otros hostings (especifique):	Servicios administrados (especificar): <input type="checkbox"/> Servicios de seguridad de sistemas <input type="checkbox"/> Soporte de TI <input type="checkbox"/> Seguridad física <input type="checkbox"/> Sistema de administración de terminales <input type="checkbox"/> Otros servicios (especificar):	Procesamiento de pago: <input type="checkbox"/> POS/tarjeta presente <input type="checkbox"/> Internet/comercio electrónico <input type="checkbox"/> MOTO/Centro de llamadas <input type="checkbox"/> ATM <input type="checkbox"/> Otro procesamiento (especifique):
<input type="checkbox"/> Administración de cuentas	<input type="checkbox"/> Fraude y reintegro de cobros	<input type="checkbox"/> Conmutador/Puerta de enlace de pagos
<input type="checkbox"/> Servicios administrativos	<input type="checkbox"/> Procesamiento del emisor	<input type="checkbox"/> Servicios prepagados
<input type="checkbox"/> Administración de facturación	<input type="checkbox"/> Programas de lealtad	<input type="checkbox"/> Administración de registros
<input type="checkbox"/> Compensación y liquidación	<input type="checkbox"/> Servicios de comerciantes	<input type="checkbox"/> Pagos de impuestos/gubernamentales
<input type="checkbox"/> Proveedor de red <input type="checkbox"/> Otros (especifique):		

Proporcione una explicación breve de las razones por las que no se incluyeron servicios marcados en la evaluación:

Parte 2b. Descripción del negocio de tarjeta de pago

Describa de qué forma y en qué capacidad almacena, procesa y/o transmite su empresa los datos de titulares de tarjetas.

Describa de qué forma y en qué capacidad su empresa está involucrada o tiene la capacidad de influir en la seguridad de los datos de titulares de tarjetas.

Parte 2c. Ubicaciones

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

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. Aplicaciones 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	
			<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?

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

Sí No

Parte 2f. Proveedores de servicio externos

<p>¿Su empresa tiene una relación con un Integrador o revendedor certificado (QIR) con el propósito de que se validen los servicios?</p> <p>En caso de ser Sí:</p> <p>Nombre de la empresa QIR:</p> <p>Nombre individual del QIR:</p> <p>Descripción de los servicios proporcionados por QIR:</p>	<p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>
---	--

Parte 2f. Proveedores de servicio externos (Continuación)

<p>¿Su empresa mantiene relaciones 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.) a los fines de validar los servicios?</p>	<p><input type="checkbox"/> Sí <input type="checkbox"/> No</p>
---	--

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. Resumen de los requisitos probados

Para cada uno de los requisitos de las PCI DSS, seleccione una de las siguientes opciones:

- **Completo:** el requisito y todos los subrequisitos se evaluaron para ese requisito, y no se marcaron subrequisitos como “No probado” o “No corresponde” en el SAQ.
- **Parcial :** un subrequisito, o más, de ese requisito se marcaron como “No probado” o “No corresponde” en el SAQ.
- **Ninguno:** todos los subrequisitos de ese requisito se marcaron como “No probado” y/o “No corresponde” en el SAQ.

En el caso de todos los requisitos identificados como “Parcial” o “Ninguno”, proporcione detalles en la columna “Justificación del enfoque”, incluidos:

- Detalles de los subrequisitos específicos que se marcaron como “No probado” y/o “No corresponde” en el SAQ.
- La razón por la que los subrequisitos no se probaron o no eran aplicables

Nota: Se debe completar una tabla para cada servicio que se abarca en este AOC. En el sitio web del PCI SSC, se encuentran disponibles copias adicionales de esta sección.

Nombre del servicio evaluado:				
Requisito de las PCI DSS	Detalles del requisito evaluado			
	Completo	Parcial	Ninguno	Justificación del enfoque (Obligatorio en el caso de las respuestas “Parcial” y “Ninguno”. Identifique cuáles son los subrequisitos que no se probaron y la razón).
Requisito 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requisito 12:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Anexo A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Anexo A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Sección 2: Cuestionario de autoevaluación D paraproveedores de servicios

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

Fecha de realización de la autoevaluación:

Desarrolle y mantenga redes y sistemas seguros

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

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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	No probado
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?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se corresponde el diagrama actual de la red con las normas de configuración de firewalls?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	¿Hay grupos, funciones y responsabilidades asignados y documentados para una administración lógica de los componentes de la red en las normas de configuración del firewall y router?	<input type="checkbox"/>	<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?	<input type="checkbox"/>	<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?	<input type="checkbox"/>	<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 estos, por lo menos, cada seis meses?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Se revisan los conjuntos de reglas del firewall y router, por lo menos, cada seis meses?	<input type="checkbox"/>	<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	No probado
1.2 ¿Restringen las configuraciones para firewalls y routers las conexiones entre redes no confiables y cualquier sistema en el entorno de los datos de titulares de tarjeta de la manera siguiente? Nota: Una “red no confiable” es toda red externa a las redes que pertenecen a la entidad en evaluación o que excede la capacidad de control o administración de la entidad.						
1.2.1 (a) ¿Está restringido el tránsito entrante y saliente a la cantidad necesaria para el entorno de los datos de titulares de tarjetas?	<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"/>	<input type="checkbox"/>
(b) ¿Se niega todo el resto del tránsito entrante o saliente (por ejemplo, mediante la utilización de una declaración explícita “negar todos” o una negación implícita después de una declaración de permiso)?	<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"/>	<input type="checkbox"/>
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"/>	<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"/>	<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	No probado
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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>
1.3.6	¿Se colocaron los componentes del sistema que almacenan datos de titulares de tarjetas (como una base de datos) en una zona de red interna, segregada desde un DMZ y otras redes no confiables?	<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"/>	<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	No probado
1.3.7 (a) ¿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"/>	<input type="checkbox"/>
(b) ¿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"/>	<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"/>	<input type="checkbox"/>
(d) ¿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"/>	<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	No probado
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"/>	<input type="checkbox"/>

Requisito 2: No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
2.1 (a) ¿Se cambian siempre los valores predeterminados por el proveedor antes de instalar un sistema en la red? <i>Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS (puntos de venta), las aplicaciones de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.</i>	<ul style="list-style-type: none"> 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"/>	<input type="checkbox"/>
(b) ¿Se eliminan o desactivan las cuentas predeterminadas que no son necesarias antes de instalar un sistema en la red?	<ul style="list-style-type: none"> 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"/>	<input type="checkbox"/>
2.1.1 Para entornos con tecnología inalámbrica conectados al entorno de datos del titular de la tarjeta o a la transmisión de datos de los titulares de tarjeta, ¿se cambian los valores predeterminados de la siguiente manera?						
(a) ¿Se cambian las claves de cifrado predeterminadas al momento de la instalación, y se cambian cada vez que una persona que tenga conocimiento de éstas cesa en sus funciones o se traslada a otro cargo en la empresa?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Revisar la documentación del proveedor Entrevistar al personal 	<input type="checkbox"/>	<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	No probado
(b) ¿Se cambian las cadenas comunitarias SNMP predeterminadas en los dispositivos inalámbricos en la instalación?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Entrevistar al personal ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Se cambian las contraseñas/frases de contraseña predeterminadas en los puntos de acceso en la instalación?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) ¿Se actualiza el firmware de los dispositivos inalámbricos a los efectos de admitir el cifrado sólido para la autenticación y la transmisión en redes inalámbricas?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) ¿Se cambian otros valores de seguridad de sistemas inalámbricos predeterminados por los proveedores, si corresponde?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Revisar la documentación del proveedor ▪ Examinar las configuraciones del sistema 	<input type="checkbox"/>	<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	No probado
(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"/>	<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"/>	<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"/>	<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	No probado
(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"/>	<input type="checkbox"/>
2.2.1 (a) ¿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"/>	<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"/>	<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	No probado
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"/>	<input type="checkbox"/>
(e) ¿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"/>	<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 usa SSL/TLS temprana, se debe completar 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"/>	<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	No probado	
2.2.4	(a) ¿Tienen conocimiento los administradores del sistema y/o el personal que configura los componentes del sistema de los parámetros de configuración de seguridad comunes correspondientes a dichos componentes del sistema?	▪ Entrevistar al personal	<input type="checkbox"/>				
	(b) ¿Están incluidos los parámetros de configuración de seguridad del sistema en las normas de configuración de sistemas?	▪ Revisar las normas de configuración del sistema	<input type="checkbox"/>				
	(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"/>				
2.2.5	(a) ¿Se eliminaron todas las funcionalidades innecesarias, tales como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios?	▪ Examinar los parámetros de seguridad en los componentes del sistema	<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"/>				
	(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"/>				

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
2.3 ¿Se cifró el acceso administrativo que no es de consola de la siguiente manera? Nota: Cuando se usa SSL/TLS temprana, se debe completar los requisitos establecidos en el Anexo A2.						
(a) ¿La totalidad del acceso administrativo que no es de consola se cifra con criptografía sólida, y se invoca un método de cifrado sólido antes de que se solicite una contraseña de administrador?	<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"/>	<input type="checkbox"/>
(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"/>	<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"/>	<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"/>	<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	No probado
2.4 (a) ¿Se conserva un inventario de los componentes del sistemas que se encuentran dentro del alcance de las PCI DSS, incluida una lista de componentes del hardware y el software con una descripción de la función/el uso de cada uno?	<ul style="list-style-type: none"> Examinar el inventario del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se mantiene actualizado el inventario documentado?	<ul style="list-style-type: none"> Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.5 ¿Las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad <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"/>	<input type="checkbox"/>
2.6 ¿Si es un proveedor de hosting compartido, configuró los sistemas para proteger cada entorno de hosting de la entidad (y de su cliente) y los datos de los titulares de tarjetas? <i>Consulte el Anexo A1: Requisitos adicionales de las PCI DSS para los proveedores de hosting compartido, para enterarse de los requisitos específicos que se deben cumplir.</i>	<ul style="list-style-type: none"> Complete los procedimientos de prueba del Anexo A1 	<input type="checkbox"/>	<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	No probado
3.1 ¿Están implementados los procedimientos, los procesos y las políticas para la retención y eliminación de datos de la siguiente manera?						
(a) ¿Está el período de almacenamiento de datos y el tiempo de retención limitado a la cantidad exigida por los requisitos legales, reglamentarios y del negocio?	<ul style="list-style-type: none"> Revisar los procedimientos y las políticas de retención y eliminación de datos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Hay implementados procesos definidos que permitan la eliminación segura de datos de titulares de tarjetas cuando ya no son necesarios por motivos legales, reglamentarios o del negocio?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal Examinar los mecanismos de eliminación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Existen requisitos específicos de retención para los datos de titulares de tarjetas? <i>Por ejemplo, los datos de los titulares de tarjetas que se retendrán durante un período X por razones de negocio.</i>	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal Examinar los requisitos de retención 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) ¿Existe un proceso trimestral para la identificación y eliminación, de manera segura, de los datos del titular de la tarjeta almacenados que excedan los requisitos de retención definidos?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal Observar los procesos de eliminación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) ¿Reúnen todos los datos de titulares de tarjetas los requisitos definidos en la política de retención de datos?	<ul style="list-style-type: none"> Examinar los archivos y los registros del sistema 	<input type="checkbox"/>	<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	No probado
3.2	(a) En el caso de los emisores de tarjetas y/o las empresas que respaldan servicios de emisión y almacenan datos confidenciales de autenticación, ¿existe una justificación de negocio para el almacenamiento de datos confidenciales de autenticación?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal Revisar la justificación de negocio documentada 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) En el caso de los emisores y/o las empresas que respaldan los servicios de emisión y almacenan datos de autenticación confidenciales: ¿Están asegurados los datos?	<ul style="list-style-type: none"> Examinar los almacenamientos de datos y los archivos de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Para todas las demás entidades: ¿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"/>	<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)?						

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
<p>3.2.1 ¿No se almacena el contenido completo de pista de la banda magnética (ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo)?</p> <p><i>Estos datos se denominan alternativamente, pista completa, pista, pista 1, pista 2 y datos de banda magnética.</i></p> <p>Nota: En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética:</p> <ul style="list-style-type: none"> • El nombre del titular de la tarjeta. • Número de cuenta principal (PAN). • Fecha de vencimiento. • Código de servicio <p><i>Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.</i></p>	<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"/>	<input type="checkbox"/>
<p>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)?</p>	<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"/>	<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	No probado
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"/>	<input type="checkbox"/>
3.3	<p>¿Está oculto el PAN cuando aparece (los primeros seis y los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda verlo completo como se indica a continuación?</p> <p>Nota: Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, requisitos legales o de las marcas de las tarjetas de pago para los recibos de POS [puntos de venta]).</p>	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Revisar las funciones que necesitan acceso a las vistas del PAN completo ▪ Examinar las configuraciones del sistema ▪ Observar las vistas del PAN 	<input type="checkbox"/>	<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	No probado
<p>3.4 ¿Se hace el PAN ilegible en cualquier lugar donde se almacene (incluidos repositorios de datos, medios digitales portátiles, medios de copia de seguridad y registros de auditoría) utilizando cualquiera de los siguientes métodos?</p> <ul style="list-style-type: none"> ▪ Valores hash de una vía basados en cifrado sólido (el hash debe ser de todo el PAN). ▪ Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN) ▪ Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura). ▪ Criptografía sólida con procesos y procedimientos asociados para la gestión de claves. <p>Nota: Para una persona malintencionada sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.</p>	<ul style="list-style-type: none"> ▪ Examinar la documentación del proveedor ▪ Examinar los depósitos de datos ▪ Examinar los medios extraíbles ▪ Examinar los registros de auditoría, incluidos los registros de aplicación de pago 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>3.4.1 ¿Cuándo se utiliza el cifrado de discos (en lugar del cifrado de bases de datos a nivel de archivo o columna), se administra el acceso de la siguiente manera?</p> <p>Nota: Este requisito se aplica, además de todos los otros requisitos de gestión de cifrado y de claves de PCI DSS.</p>						
<p>(a) ¿Se administra un acceso lógico a los sistemas de archivos cifrados en forma independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red)?</p>	<ul style="list-style-type: none"> ▪ Examinar las configuraciones del sistema ▪ Observar el proceso de autenticación 	<input type="checkbox"/>	<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	No probado
(b) ¿Se almacenan de manera segura las claves criptográficas (por ejemplo, se almacenen en medios extraíbles protegidos adecuadamente con controles sólidos de acceso)?	<ul style="list-style-type: none"> Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Se cifran los datos de titulares de tarjetas que se encuentran en medios extraíbles donde quiera que se almacenen? <i>Nota: Si no se utiliza el cifrado de disco para cifrar medios extraíbles, los datos almacenados en estos medios deberán quedar ilegibles mediante algún otro método.</i>	<ul style="list-style-type: none"> Examinar las configuraciones del sistema Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5 ¿Se utilizan claves para asegurar los datos de titulares de tarjetas contra divulgación o uso indebido de la siguiente manera? <i>Nota: Este requisito se aplica a las claves utilizadas para cifrar datos del titular de la tarjeta almacenados y para claves de cifrado de claves utilizadas para proteger las claves de cifrado de datos. Dichas claves de cifrado de claves deben ser tan sólidas como las claves de cifrado de datos, como mínimo.</i>						
3.5.1 <i>Solo para proveedores de servicios:</i> ¿Se mantiene una descripción documentada de la arquitectura criptográfica que incluye?: <ul style="list-style-type: none"> Detalles de todos los algoritmos, protocolos y claves usados para la protección de los datos del titular de la tarjeta, incluidos la solidez de la clave y la fecha de vencimiento, Descripción del uso clave para cada tecla, ¿Inventario de cualquier HSM y otros SCD usados para la gestión de claves? <i>Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.</i>	<ul style="list-style-type: none"> Entrevistar al personal Revisar la documentación 	<input type="checkbox"/>	<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	No probado
3.5.2	¿Se restringe el acceso a las claves de cifrado al número mínimo de custodios necesarios?	<ul style="list-style-type: none"> Examinar las listas de acceso de usuario 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	<p>¿Se utilizan claves criptográficas secretas y privadas para cifrar/descifrar los datos del titular de la tarjeta en una (o más) de las siguientes formas en todo momento?</p> <ul style="list-style-type: none"> Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS) Como, al menos, dos claves o componentes de la clave completos de acuerdo con los métodos aceptados por la industria. <p>Nota: No es necesario guardar las claves públicas de esta manera.</p>	<ul style="list-style-type: none"> Revisar los procedimientos documentados Examinar las configuraciones del sistema y las ubicaciones de almacenamiento de claves, incluidas las claves de cifrado de claves. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5.4	¿Se almacenan las claves criptográficas en la menor cantidad de ubicaciones posibles?	<ul style="list-style-type: none"> Examinar las ubicaciones de almacenamiento de claves Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6	(a) ¿Se documentan e implementan por completo todos los procesos y procedimientos de administración de claves para las claves criptográficas utilizadas en el cifrado de los datos de titulares de tarjetas?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) <i>Solo para proveedores de servicio:</i> ¿Si se comparten claves con clientes para la transmisión o almacenamiento de datos de titulares de tarjetas, se proporciona documentación a los clientes que incluya directrices sobre cómo transmitir, almacenar y actualizar de manera segura las claves del cliente de conformidad con los requisitos 3.6.1 a 3.6.8 que aparecen a continuación?	<ul style="list-style-type: none"> Revisar la documentación proporcionada a los clientes 	<input type="checkbox"/>	<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	No probado
	(c) ¿Se implementan los procesos y procedimientos de administración de claves de modo que requieran lo siguiente?						
3.6.1	¿Incluyen los procedimientos de claves criptográficas la generación de claves criptográficas sólidas?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Observar los procedimientos de generación de claves 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	¿Incluyen los procedimientos de claves criptográficas la distribución de claves criptográficas seguras?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Observar el método de distribución de claves 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	¿Incluyen los procedimientos de claves criptográficas el almacenamiento de claves criptográficas seguro?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Observar el método de almacenamiento seguro de claves 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	¿Incluyen los procedimientos de claves criptográficas los cambios de claves criptográficas por claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que una clave dada haya producido cierta cantidad de texto cifrado), según lo define el proveedor de la aplicación relacionada o el responsable de las claves, y basándose en las mejores prácticas y recomendaciones de la industria (por ejemplo, NIST Special Publication 800-57)?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5	(a) ¿Incluyen los procedimientos de claves criptográficas el retiro o reemplazo (por ejemplo, mediante archivo, destrucción y/o revocación) de claves criptográficas cuando se haya debilitado la integridad de la clave (por ejemplo, salida de la empresa de un empleado con conocimiento de una clave en texto claro)?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Entrevistar al personal 	<input type="checkbox"/>	<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	No probado
(b) ¿Incluyen los procedimientos de claves criptográficas el reemplazo de claves cuando se sepa o sospeche que están comprometidas?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Si se retienen las claves criptográficas retiradas o reemplazadas, ¿solo se utilizan estas claves para operaciones de descifrado/verificación y no para operaciones de cifrado?	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.6 Si se usan operaciones manuales de administración de claves criptográficas de texto claro, ¿los procedimientos de clave criptográficas incluyen control doble y conocimiento dividido de las claves criptográficas como se indica? <ul style="list-style-type: none"> ¿Los procedimientos de conocimiento dividido requieren que los componentes clave estén bajo el control de, al menos, dos personas que solo tengan conocimiento de los componentes de su propia clave? ¿Los procedimientos de control doble de claves requieren, al menos, dos personas para realizar las operaciones de administración de claves y que ninguna tenga acceso al material de autenticación de la otra (por ejemplo, contraseñas o claves)? <p>Nota: Los ejemplos de operaciones manuales de gestión de claves incluyen, entre otros: generación, transmisión, carga, almacenamiento y destrucción de claves.</p>	<ul style="list-style-type: none"> Revisar los procedimientos de administración de claves Entrevistar al personal y/o Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.7 ¿Incluyen los procedimientos de claves criptográficas la prevención de sustitución no autorizada de claves criptográficas?	<ul style="list-style-type: none"> Revisar los procedimientos Entrevistar al personal y/o Observar los procesos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8 ¿Se requiere que los custodios de claves criptográficas reconozcan formalmente (ya sea de manera escrita o electrónica) que entienden y aceptan sus responsabilidades como custodios de las claves?	<ul style="list-style-type: none"> Revisar los procedimientos Revisar la documentación u otra evidencia 	<input type="checkbox"/>	<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	No probado
3.7	<p>¿Las políticas de seguridad y los procedimientos operativos para la protección de los datos de titulares de tarjetas</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"/>	<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	No probado
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 usa SSL/TLS temprana, se debe completar los requisitos establecidos en el Anexo A2.</i> <i>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"/>	<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"/>	<input type="checkbox"/>
(c) ¿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"/>	<input type="checkbox"/>
(d) ¿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"/>	<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	No probado
	(e) Para las implementaciones de TLS, ¿está TLS habilitado al transmitir o recibir los datos del titular de la tarjeta? <i>Por ejemplo, para implementaciones basadas en explorador:</i> <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"/>	<input type="checkbox"/>
4.1.1	¿Se aplican las mejores prácticas de la industria para implementar el cifrado sólido para la autenticación y transmisión para redes inalámbricas de transmisión de datos de los titulares de tarjeta o conectados con el entorno de datos del titular de la tarjeta?	<ul style="list-style-type: none"> ▪ Revisar las normas documentadas ▪ Revisar redes inalámbricas ▪ Examinar los parámetros de configuración del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2	(a) ¿Se hacen ilegibles o se aseguran los números PAN con criptografía sólida siempre que se envían a través de tecnologías de mensajería de usuario final (por ejemplo, correo electrónico, mensajería instantánea, SMS, chat, etc.)?	<ul style="list-style-type: none"> ▪ Observar los procesos ▪ Revisar las transmisiones salientes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se implementaron políticas que especifiquen que no se deben enviar números PAN sin protección a través de tecnologías de mensajería del usuario final?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.3	¿Las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de datos de titulares de tarjeta <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"/>	<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	No probado
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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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	No probado
	(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"/>	<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>Nota: Las soluciones de antivirus se pueden desactivar temporalmente, pero solo si existe una necesidad técnica legítima como en el caso de la autorización de la gerencia en casos particulares. Si es necesario desactivar la protección de antivirus por un motivo específico, se debe contar con una autorización formal. Es posible que sea necesario implementar medidas de seguridad adicionales en el período en que no esté activa la protección de antivirus.</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"/>	<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"/>	<input type="checkbox"/>

Requisito 6: Desarrolle y mantenga 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	No probado
<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 se deben basar en las mejores prácticas de la industria y en el posible impacto. 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"/>	<input type="checkbox"/>
<p>6.2 (a) ¿Están todos los programas de software y componentes del sistema protegidos de las vulnerabilidades conocidas mediante parches de seguridad instalados proporcionados por los proveedores?</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"/>	<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	No probado
(b) ¿Se instalan parches de seguridad crítica en un lapso de un mes contado a partir de su fecha de lanzamiento? <i>Nota: Los parches de seguridad críticos se deben identificar de conformidad con el proceso de clasificación de riesgos definido en el Requisito 6.1.</i>	<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"/>	<input type="checkbox"/>
6.3 (a) ¿Se basan los procesos de desarrollo de software en las normas y/o mejores prácticas de la industria?	<ul style="list-style-type: none"> Revisar los procesos de desarrollo de software Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se incluye la seguridad de la información en todo el ciclo de vida de desarrollo del software?	<ul style="list-style-type: none"> Revisar los procesos de desarrollo de software Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Se desarrollan aplicaciones de software de conformidad con las PCI DSS (por ejemplo, autenticación y registros seguros)?	<ul style="list-style-type: none"> Revisar los procesos de desarrollo de software Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) ¿Aseguran los procesos de desarrollo de software lo siguiente en los Requisitos 6.3.1 - 6.3.2?						
6.3.1 ¿Se eliminan las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas antes de que las aplicaciones se activen o se pongan a disposición de los clientes?	<ul style="list-style-type: none"> Revisar los procesos de desarrollo de software Entrevistar al personal 	<input type="checkbox"/>	<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	No probado
<p>6.3.2 ¿Se revisan todos los códigos personalizados (ya sea utilizando procesos manuales o automatizados) antes de ponerlos a disposición de la producción o los clientes a fin de identificar cualquier vulnerabilidad potencial en la codificación de la siguiente manera?</p> <ul style="list-style-type: none"> ▪ ¿Está la revisión de los cambios en los códigos a cargo de personas que no han creado el código y que tienen conocimiento de técnicas de revisión de código y prácticas de codificación segura? ▪ ¿Las revisiones de los códigos garantizan que el código se desarrolle de acuerdo con las directrices de codificación segura? ▪ ¿Se implementan las correcciones pertinentes antes del lanzamiento? ▪ ¿La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento? <p>Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema. Las revisiones de los códigos pueden ser realizadas por terceros o por personal interno con conocimiento. Las aplicaciones web también están sujetas a controles adicionales a los efectos de tratar las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las PCI DSS.</p>	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos ▪ Entrevistar al personal ▪ Examinar los cambios recientes y los registros de cambios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>6.4 ¿Se siguen los procesos y procedimientos de control de cambios para todos los cambios de los componentes del sistema a efectos de incluir lo siguiente?</p>						

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
6.4.1	(a) ¿Están separados los entornos de prueba/desarrollo del entorno de producción?	<ul style="list-style-type: none"> Revisar los procesos y procedimientos de control de cambio Examinar las configuraciones del dispositivo de red y la documentación de red 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Está implementado el control de acceso para cumplir con la separación entre los entornos de prueba/desarrollo y el entorno de producción?	<ul style="list-style-type: none"> Revisar los procesos y procedimientos de control de cambio Examinar los parámetros de control de acceso 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2	¿Existe una separación de funciones entre el personal asignado a los entornos de desarrollo/prueba y los asignados al entorno de producción?	<ul style="list-style-type: none"> Revisar los procesos y procedimientos de control de cambio Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3	¿ No se utilizan los datos de producción (PAN activos) para las pruebas ni para el desarrollo?	<ul style="list-style-type: none"> Revisar los procesos y procedimientos de control de cambio Observar los procesos Entrevistar al personal Examinar los datos de la prueba 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4	¿Se eliminan los datos de las pruebas y las cuentas de los componentes del sistema antes de activar los sistemas de producción?	<ul style="list-style-type: none"> Revisar los procesos y procedimientos de control de cambio Observar los procesos Entrevistar al personal Examinar los sistemas de producción 	<input type="checkbox"/>	<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	No probado	
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"/>				
	(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"/>				
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"/>				
6.4.5.3	(a) ¿Hay una prueba de funcionalidad a fin de verificar que el cambio no incide de forma adversa 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"/>				
	(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"/>				

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
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"/>	<input type="checkbox"/>
6.4.6	<p>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?</p> <p>Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.</p>	<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"/>	<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	No probado	
6.5	(a) ¿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"/>				
	(b) ¿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"/>				
	(c) ¿Se desarrollan las aplicaciones en función de las pautas de codificación de seguridad para proteger las aplicaciones, al menos, contra las siguientes vulnerabilidades? <i>Nota: Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el 6.5.10 eran congruentes con las mejores prácticas de la industria al momento de la publicación de esta versión de las PCI DSS. Sin embargo, debido a que las mejores prácticas de la industria para la gestión de vulnerabilidades se actualizan (por ejemplo, OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), se deben utilizar las mejores prácticas actuales para estos requisitos.</i>						
6.5.1	¿Las técnicas de codificación corrigen los errores de inyección, en especial errores de inyección SQL? <i>Nota: También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.</i>	<ul style="list-style-type: none"> Examinar las políticas y los procedimientos del desarrollo de software Entrevistar al personal a cargo 	<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"/>				

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
6.5.3	¿Las técnicas de codificación corrigen el almacenamiento criptográfico no seguro?	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>
<p>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:</p>							
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"/>	<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"/>	<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	No probado
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"/>	<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"/>	<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	No probado
<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"/>	<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	No probado
6.7	<p>¿Las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones</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"/>	<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	No probado	
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?:						
	<ul style="list-style-type: none"> ▪ ¿Existe una política escrita para el control de acceso que incorpora lo siguiente? <ul style="list-style-type: none"> • Definición de las necesidades de acceso y asignación de privilegios de cada función. • Restricción de acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo. • Asignación de acceso según la tarea, la clasificación y la función de cada persona. • Aprobación documentada (por escrito o electrónicamente) de las partes autorizadas para todos los accesos, que incluye la lista de los privilegios específicos aprobados. 	<ul style="list-style-type: none"> ▪ Examinar la política de control de acceso escrita 	<input type="checkbox"/>				
7.1.1	¿Están definidas las necesidades de acceso de cada función, incluso lo siguiente? <ul style="list-style-type: none"> ▪ Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. ▪ Nivel de privilegio necesario (por ejemplo, usuario, administrador, etc.) para acceder a los recursos. 	<ul style="list-style-type: none"> ▪ Examinar las funciones y las necesidades de acceso 	<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	No probado
7.1.2	<p>¿El acceso a las identificaciones de usuario con privilegios está restringido según se indica a continuación?</p> <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"> ▪ 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"/>	<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"> ▪ Entrevistar a la administración ▪ Revisar las identificaciones de los usuarios 	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>
7.2	¿Se implementó un sistema de control de acceso para los componentes del sistema que restrinja el acceso basado en la necesidad del usuario de conocer y que se configure para “negar todo”, salvo que se permita específicamente, de la siguiente manera?						
7.2.1	¿Se implementaron sistemas de control de acceso en todos los componentes del sistema?	<ul style="list-style-type: none"> ▪ Revisar la documentación del proveedor ▪ Examinar los parámetros de configuración 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	¿Están configurados los sistemas de control de acceso a los efectos de hacer cumplir los privilegios asignados a los individuos sobre la base de la clasificación de la tarea y la función?	<ul style="list-style-type: none"> ▪ Revisar la documentación del proveedor ▪ Examinar los parámetros de configuración 	<input type="checkbox"/>	<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	No probado
7.2.3	¿Poseen los sistemas de control de acceso un ajuste predeterminado de “negar todos”?	<ul style="list-style-type: none"> ▪ Revisar la documentación del proveedor ▪ Examinar los parámetros de configuración 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.3	¿Las políticas de seguridad y los procedimientos operativos para la restricción del acceso a los datos de titulares de tarjetas <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"/>	<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	No probado
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"/>	<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"/>	<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"/>	<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"/>	<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	No probado
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"/>	<input type="checkbox"/>
	(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"/>	<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"/>	<input type="checkbox"/>
	(b) <i>Solo para proveedores de servicios:</i> ¿Se bloquean temporalmente las contraseñas de usuarios no consumidores después de no más de seis intentos de acceso no válidos?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Revisar la documentación Observar los procesos 	<input type="checkbox"/>	<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"/>	<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"/>	<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	No probado
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"/>	<input type="checkbox"/>
8.2.1	(a) ¿La criptografía sólida se utiliza para dejar ilegibles todas las credenciales de autenticación (como contraseñas/frases) 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"/>	<input type="checkbox"/>
	(b) <i>Solo para proveedores de servicios:</i> ¿La criptografía sólida se utiliza para dejar ilegibles todas las credenciales de autenticación de los usuarios no consumidores (como contraseñas/frases) durante la transmisión y el almacenamiento en todos los componentes del sistema?	<ul style="list-style-type: none"> ▪ Observar los archivos de contraseña ▪ Observar las transmisiones de datos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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"/>	<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	No probado
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"/>	<input type="checkbox"/>
	(b) <i>Solo para proveedores de servicio:</i> ¿Se requiere que las contraseñas de los usuarios no consumidores cumplan con los siguientes requisitos de extensión y complejidad mínimas? <ul style="list-style-type: none"> • Longitud de contraseña mínima de siete caracteres • Combinación de caracteres numéricos y alfabéticos 	<ul style="list-style-type: none"> ▪ Revisar la documentación del cliente/usuario ▪ Observar los procesos internos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.4	(a) ¿Se cambian las contraseñas/frases de 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"/>	<input type="checkbox"/>
	(b) <i>Solo para proveedores de servicios:</i> ¿Se requiere que las contraseñas de usuarios no consumidores se cambien periódicamente y que estos reciban orientación sobre cuándo, y bajo cuáles circunstancias, se deben cambiar las contraseñas?	<ul style="list-style-type: none"> ▪ Revisar la documentación del cliente/usuario ▪ Observar los procesos internos 	<input type="checkbox"/>	<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	No probado
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"/>	<input type="checkbox"/>
	(b) <i>Solo para proveedores de servicios:</i> ¿Se requiere que las nuevas contraseñas de usuarios no consumidores sean diferentes de las últimas cuatro contraseñas que utilizaron?	<ul style="list-style-type: none"> Revisar la documentación del cliente/usuario Observar los procesos internos 	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>
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>						

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
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><i>Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.</i></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"/>	<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"/>	<input type="checkbox"/>
8.4	(a) ¿Se documentan y comunican los procedimientos y las políticas de autenticación a todos los usuarios?	<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"/>	<input type="checkbox"/>
	(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"/>	<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	No probado
8.5	<p>¿Se prohíben las cuentas y contraseñas grupales, compartidas o genéricas u otros métodos de autenticación, de la siguiente manera?</p> <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"/>	<input type="checkbox"/>
8.5.1	<p><i>Solo para proveedores de servicios:</i> ¿Los proveedores de servicios que tengan acceso a las instalaciones del cliente (por ejemplo, para tareas de soporte de los sistemas de POS o de los servidores) deben usar una credencial de autenticación exclusiva (como una contraseña/frase) para cada cliente?</p> <p>Nota: El objetivo de este requisito no es aplicarlo a los proveedores de servicios de hosting compartido que acceden a su propio entorno de hosting, donde se alojan numerosos entornos de clientes.</p>	<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"/>	<input type="checkbox"/>
8.6	<p>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?</p> <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"/>	<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	No probado
8.7 ¿Se restringen todos los accesos a cualquier base de datos que contenga datos del titular de la tarjeta (que incluye acceso por parte de aplicaciones, administradores y todos los otros usuarios) de la siguiente manera?						
(a) ¿Realizan los usuarios las actividades relacionadas con la base de datos, tales como el acceso, las consultas y otras acciones (por ejemplo, mover, copiar, eliminar) solo a través de métodos de programación (por ejemplo, a través de procedimientos almacenados)?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de autenticación de la base de datos ▪ Examinar los parámetros de configuración de la base de datos y la aplicación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se limita el acceso directo o las consultas de usuarios a la base de datos a los administradores de la base de datos?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de autenticación de la base de datos ▪ Examinar los parámetros de control de acceso a la base de datos ▪ Examinar los parámetros de configuración de la aplicación de la base de datos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) ¿Solo pueden las aplicaciones (y no usuarios ni otros procesos) utilizar las ID de aplicaciones con acceso a la base de datos?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de autenticación de la base de datos ▪ Examinar los parámetros de control de acceso a la base de datos ▪ Examinar los parámetros de configuración de la aplicación de la base de datos 	<input type="checkbox"/>	<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	No probado
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"/>	<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	No probado
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"/>	<input type="checkbox"/>
9.1.1	(a) ¿Hay cámaras de video y/u otros mecanismos de control de acceso (o ambos) para supervisar el acceso físico de personas a áreas confidenciales? <i>Nota: "Áreas confidenciales" hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan procesos o transmitan datos de titulares de tarjetas. No se incluyen las áreas públicas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.</i>	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Observar los mecanismos de supervisión física Observar las funciones de seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se protegen las cámaras de video y/u otros mecanismos de control de acceso (o ambos) contra alteraciones y desactivaciones?	<ul style="list-style-type: none"> Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) ¿Se revisan y correlacionan con otras entradas los datos recogidos de cámaras de video y/u otros mecanismos de control de acceso?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal de seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) ¿Se almacenan los datos recogidos de cámaras de video y/u otros mecanismos de control de acceso durante por lo menos tres meses, a menos que lo restrinja la ley?	<ul style="list-style-type: none"> Revisar los procesos de retención de datos Observar el almacenamiento de datos Entrevistar al personal de seguridad 	<input type="checkbox"/>	<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	No probado
9.1.2	<p>¿Hay implementados controles físicos o lógicos para restringir el acceso a conexiones de red de acceso público?</p> <p><i>Por ejemplo, las conexiones de red en áreas públicas y en las que pueden acceder los visitantes se pueden inhabilitar y habilitar solo cuando el acceso a la red se autoriza explícitamente. De forma alternativa, se pueden implementar procesos para asegurarse de que los visitantes estén acompañados en todo momento en áreas con conexiones de red activas.</i></p>	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal Observar las ubicaciones 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.3	<p>¿Se encuentra restringido el acceso físico a puntos de acceso, puertas de enlace, dispositivos portátiles, hardware de redes/comunicaciones y líneas de telecomunicaciones?</p>	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal Observar los dispositivos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.2	<p>(a) ¿Se desarrollan procedimientos que permiten distinguir fácilmente entre los empleados y los visitantes, que incluyen lo siguiente?</p> <ul style="list-style-type: none"> Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). Cambiar los requisitos de acceso. Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación). <p><i>A los fines del Requisito 9, "empleados" se refiere a personal de tiempo completo y parcial, personal temporal, contratistas y consultores que estén físicamente presentes en las instalaciones de la entidad. "Visitante" se define como proveedor, invitado de algún empleado, personal de servicio o cualquier persona que necesite ingresar a las instalaciones durante un tiempo no prolongado, generalmente no más de un día.</i></p>	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Entrevistar al personal Observar los métodos de identificación (por ejemplo, placas de identificación) Observar los procesos de visita 	<input type="checkbox"/>	<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	No probado
	(b) ¿Los métodos de identificación (como placas de identificación) identifican de manera clara a los visitantes y establecen una clara diferencia entre empleados y visitantes?	<ul style="list-style-type: none"> Observar los métodos de identificación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(e) ¿Está limitado el acceso al sistema de placas de identificación al personal autorizado?	<ul style="list-style-type: none"> Observar los controles físicos y de acceso para el sistema de placas de identificación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.3	<p>¿El acceso físico a las áreas confidenciales está controlado para los empleados, de la siguiente manera?</p> <ul style="list-style-type: none"> ¿El acceso está autorizado y se otorga según el trabajo de cada persona? ¿El acceso se cancela de inmediato una vez el empleado queda cesante? Una vez finalizado el empleo, ¿se devuelven o desactivan todos los mecanismos de acceso físicos, como claves, tarjetas de acceso, etc.? 	<ul style="list-style-type: none"> Entrevistar al personal Examinar las listas de control de acceso Observar a los empleados Comparar las listas de los empleados cesantes con las listas de control de acceso 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4	¿Se gestiona la identificación y el acceso de los visitantes de la siguiente manera?						
9.4.1	¿Los visitantes reciben autorización antes de ingresar en las áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y están acompañados en todo momento?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Observar los procesos de los visitantes, incluido el control del acceso Entrevistar al personal Observar los visitantes y el uso de la placa de identificación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.2	(a) ¿Se identifican los visitantes y se les entrega una placa u otro elemento de identificación que permite diferenciar claramente entre empleados y visitantes?	<ul style="list-style-type: none"> Observar el uso de la placa de identificación de los empleados y los visitantes Examinar la identificación 	<input type="checkbox"/>	<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	No probado
	(b) ¿Tienen vencimiento las placas de identificación de visitantes, u otro tipo de identificación?	<ul style="list-style-type: none"> Observar el proceso Examinar la identificación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.3	¿Los visitantes deben entregar la placa o la identificación antes de salir de las instalaciones o al momento del vencimiento?	<ul style="list-style-type: none"> Observar los procesos Observar los visitantes cuando abandonan las instalaciones 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.4	(a) ¿Se utiliza un registro para dar cuenta del acceso físico a las instalaciones de la empresa, así como también a las salas de informática y los centros de datos donde se guardan o se transmiten datos de titulares de tarjetas?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Examinar el registro de visitas Observar los procesos de visita Examinar la retención del registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿El registro de visitas contiene el nombre del visitante, la empresa representada, y el personal del sitio que autoriza el acceso físico?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Examinar el registro de visitas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(f) ¿Se conserva el registro de visitas durante, al menos, tres meses?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos Examinar la retención del registro de visitas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5	<p>¿Todos los medios de almacenamiento están físicamente asegurados (incluyendo, sin sentido limitativo, computadoras, medios extraíbles electrónicos, recibos en papel, informes de papel y faxes)?</p> <p><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></p>	<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"/>	<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	No probado
9.5.1	¿Se revisa la ubicación donde se almacenan las copias de seguridad, por lo menos anualmente, para confirmar que el almacenamiento es seguro?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos para la revisión de las ubicaciones de medios externas Entrevistar al personal de seguridad 	<input type="checkbox"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>
9.7.1	(a) ¿Se mantienen adecuadamente los registros de inventario de todos los medios?	<ul style="list-style-type: none"> Examinar los registros de inventario 	<input type="checkbox"/>	<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	No probado
	(b) ¿Se realizan inventarios de medios habitualmente, por lo menos una vez al año?	<ul style="list-style-type: none"> ▪ Examinar los registros de inventario ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	(a) ¿Se destruyen los medios cuando ya no sean necesarios para la empresa o por motivos legales?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos para la destrucción periódica de medios 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Hay implementada una política de destrucción de medios periódica que define los requisitos para lo siguiente? <ul style="list-style-type: none"> • Los materiales de copias en papel se deben cortar en tiras, incinerarse o convertirse en pulpa para tener la certeza de que no podrán reconstruirse. • Los contenedores de almacenamiento que se usan para los materiales que se destruirán deben estar protegidos. • Los datos del titular de la tarjeta guardados en medios electrónicos deben permanecer irrecuperables mediante un programa con la función de limpieza segura (de acuerdo con las normas aceptadas en la industria para lograr una eliminación segura) o mediante la destrucción física de los medios. 	<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"/>	<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"> ▪ Entrevistar al personal ▪ Examinar los procedimientos ▪ Observar los procesos 	<input type="checkbox"/>	<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"/>	<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	No probado
9.8.2	¿Se hacen irrecuperables los datos de titulares de tarjetas guardados en dispositivos electrónicos (por ejemplo, a través de un programa con la función de limpieza segura de acuerdo con las normas aceptadas en la industria para lograr una eliminación segura, o bien mediante la destrucción de los medios de forma física) de modo que los datos de los titulares de tarjetas no se puedan reconstruir?	<ul style="list-style-type: none"> Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	<p>¿Están protegidos los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta contra alteraciones y sustituciones?</p> <p>Nota: Este requisito rige para los dispositivos de lectura de tarjetas que se usan en transacciones (es decir, al pasar o deslizar la tarjeta) en los puntos de venta. El objetivo de este requisito no es aplicarlo a los componentes de ingreso de claves, como teclados de computadoras y teclados numéricos de POS (puntos de ventas).</p>						
(a)	¿Las políticas y los procedimientos requieren que se mantenga una lista de dichos dispositivos?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b)	¿Las políticas y los procedimientos requieren que los dispositivos se inspeccionen periódicamente para buscar intentos de alteración o sustitución?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c)	¿Las políticas y los procedimientos requieren que el personal esté capacitado para que detecten comportamientos sospechosos e informen la alteración o sustitución de dispositivos?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<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	No probado
9.9.1 (a) ¿En la lista de dispositivos se incluye lo siguiente? <ul style="list-style-type: none"> • Marca y modelo del dispositivo • Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) • Número de serie del dispositivo u otro método de identificación única 	<ul style="list-style-type: none"> ▪ Examinar la lista de dispositivos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿La lista es precisa y está actualizada?	<ul style="list-style-type: none"> ▪ Observar los dispositivos y las ubicaciones de los dispositivos y comparar con la lista 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Se actualiza la lista cuando se agregan, reubican y desactivan los dispositivos?	<ul style="list-style-type: none"> ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.2 (a) ¿Se inspeccionan periódicamente las superficies de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento)? <i>Nota: Entre los ejemplos de indicios de que un dispositivo puede haber sido alterado o sustituido, se pueden mencionar accesorios inesperados o cables conectados al dispositivo, etiquetas de seguridad faltantes o cambiadas, carcasas rotas o con un color diferente o cambios en el número de serie u otras marcas externas.</i>	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Observar los procesos de inspección y comparar con los procesos definidos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿El personal conoce los procedimientos para inspeccionar los dispositivos?	<ul style="list-style-type: none"> ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.3 ¿Está capacitado el personal para que detecten indicios de alteración o sustitución en los dispositivos?						

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
(a) ¿El material de capacitación para el personal que trabaja en los puntos de venta incluye lo siguiente? <ul style="list-style-type: none"> • Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de autorizarlos a acceder y modificar un dispositivo o solucionar algún problema. • No instalar, cambiar ni devolver dispositivos sin verificación. • Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). • Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad). 	<ul style="list-style-type: none"> ▪ Revisar los materiales de capacitación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿El personal que trabaja en los puntos de venta recibió capacitación, y conoce los procedimientos que se emplean en la detección y realización de informes en casos de indicios de alteración o sustitución de los dispositivos?	<ul style="list-style-type: none"> ▪ Entrevistar al personal en los puntos de venta 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.10 ¿Las políticas de seguridad y los procedimientos operativos para la restricción del acceso físico a los datos de titulares de tarjetas <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"/>	<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 de los titulares de las tarjetas*

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
10.1	(a) ¿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"/>	<input type="checkbox"/>
	(b) ¿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"/>	<input type="checkbox"/>
10.2	¿Se implementan pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos?						
10.2.1	Todos los usuarios acceden a los datos de titulares de tarjetas.	<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"/>	<input type="checkbox"/>
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"/>	<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"/>	<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	No probado
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"/>	<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"/>	<input type="checkbox"/>
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"/>	<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"/>	<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"/>	<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	No probado
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"/>	<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"/>	<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"/>	<input type="checkbox"/>
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"/>	<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"/>	<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"/>	<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	No probado	
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"/>				
(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"/>				
(g)	¿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"/>				
10.4.2	¿Se protegen los datos de tiempo de la siguiente manera:		<input type="checkbox"/>				
(a)	¿Se restringe el acceso a los datos de horario solo al personal con una necesidad de negocio de acceder a dichos datos?	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y los parámetros de sincronización de tiempo 	<input type="checkbox"/>				
(b)	¿Se registran, supervisan y revisan los cambios a los parámetros de hora en los sistemas críticos?	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y los parámetros y registros de sincronización de tiempo 	<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	No probado
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, se pueden cifrar estas actualizaciones con una clave simétrica, y se pueden crear listas de control de acceso que especifiquen las direcciones IP de equipos cliente a los que se proporcionarán las actualizaciones de tiempo (para evitar el uso no autorizado de servidores de hora 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"/>	<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"/>	<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"/>	<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"/>	<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	No probado
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"/>	<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"/>	<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>						

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
10.6.1 (a) ¿Están las políticas y los procedimientos escritos definidos para revisar lo siguiente, al menos, una vez al día, ya sea manualmente o con herramientas de registro? <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 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se revisan los eventos de seguridad y registros mencionados como mínimo diariamente?	<ul style="list-style-type: none"> ▪ Observar los procesos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.2 (a) ¿Están las políticas y los procedimientos escritos definidos para realizar una revisión periódica de los registros de todos los demás componentes del sistema, ya sea de forma manual o con herramientas de registros, según las políticas y estrategia de gestión de riesgos de la organización?	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos de seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se realizan las revisiones de todos los demás componentes del sistema según la política y estrategia de gestión de riesgos de la organización?	<ul style="list-style-type: none"> ▪ Revisar la documentación de evaluación de riesgo ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6.3 (a) ¿Están las políticas y los procedimientos escritos definidos para realizar 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 	<input type="checkbox"/>	<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	No probado
	(b) ¿Se realiza un seguimiento de las excepciones y anomalías?	<ul style="list-style-type: none"> Observar los procesos Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.7	(a) ¿Hay implementadas políticas y procedimientos de retención de registros de auditorías, y es necesario que se conserven los registros al menos un año, con un mínimo de disponibilidad inmediata para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad)?	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos de seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se retienen los registros de auditoría por al menos un año?	<ul style="list-style-type: none"> Entrevistar al personal Examinar los registros de auditoría 	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>
10.8	<p><i>Solo para proveedores de servicios: ¿Se implementa un proceso para la detección y la presentación de informes oportunos de fallas de los sistemas de control de seguridad críticos como sigue?:</i></p> <p>Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.</p>						

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
	(a) ¿Se implementan procesos para la detección y presentación de informes oportunas de fallas de los sistemas de control de seguridad críticos, por ejemplo, entre otros la falla de: <ul style="list-style-type: none"> • Firewalls • IDS/IPS • FIM • Antivirus • Controles de acceso físicos • Control de acceso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan) 	<ul style="list-style-type: none"> ▪ Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿La falla de un control de seguridad crítico da lugar a la generación de una alerta?	<ul style="list-style-type: none"> ▪ Observar los procesos ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.8.1	<i>Solo para proveedores de servicios: ¿Se responde a las fallas de los controles de seguridad críticos de manera oportuna, como sigue?:</i> Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.						

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
(a) ¿Se definen e implementan procesos para responder a las fallas de los controles de seguridad críticos, e incluyen?: <ul style="list-style-type: none"> • Restauración de las funciones de seguridad • Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad • Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la solución requerida para abordar la causa raíz • Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad. • Implementar controles para evitar que se vuelva a producir la causa de la falla • ¿Reanudar la supervisión de los controles de seguridad? 	<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"/>	<input type="checkbox"/>
(b) ¿Se documentan las fallas en los controles de seguridad críticos, incluido?: <ul style="list-style-type: none"> • Identificación de las causas de la falla, incluida la causa raíz • Duración (fecha y hora de inicio a fin) de la falla de seguridad • ¿Detalles de la solución requerida para abordar la causa raíz? 	<ul style="list-style-type: none"> ▪ Examinar registros de las fallas de los controles de seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.9 ¿Las políticas de seguridad y los procedimientos operativos para la supervisión de todo el acceso a los datos de titulares de tarjetas y los recursos de red <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"/>	<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	No probado
11.1 (a) ¿Hay procedimientos implementados para detectar e identificar, trimestralmente, puntos de acceso inalámbricos autorizados y no autorizados? Nota: Los métodos que se pueden utilizar en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos. Independientemente de los métodos que se utilicen, éstos deben ser suficientes para detectar e identificar cualquier dispositivo no autorizado.	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿La metodología es capaz de detectar e identificar cualquier punto de acceso inalámbrico no autorizado, incluido por lo menos lo siguiente? <ul style="list-style-type: none"> Tarjetas WLAN insertadas en los componentes del sistema; Dispositivos portátiles o móviles conectados a los componentes del sistema para crear un punto de acceso inalámbrico (por ejemplo, mediante USB, etc.); y Dispositivos inalámbricos conectados a un puerto o a un dispositivo de red. 	<ul style="list-style-type: none"> Evaluar la metodología 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(h) ¿Se realiza por lo menos trimestralmente el escaneo para identificar los puntos de acceso inalámbricos no autorizados para todos los componentes e instalaciones de sistemas?	<ul style="list-style-type: none"> Examinar el resultado de los escaneos inalámbricos recientes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(i) Si se utiliza supervisión automatizada (por ejemplo, IDS/IPS inalámbrico, NAC, etc.), ¿se configura la supervisión para que genere alertas al personal?	<ul style="list-style-type: none"> Examinar los parámetros de configuración 	<input type="checkbox"/>	<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	No probado
11.1.1	¿Se conserva un inventario de los puntos de acceso inalámbricos autorizados y una justificación comercial documentada para todos los puntos de acceso inalámbricos autorizados?	<ul style="list-style-type: none"> Examinar los registros de inventario 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.2	(a) ¿El Plan de respuesta a incidentes define y requiere una respuesta en caso de que se detecte un punto de acceso inalámbrico no autorizado?	<ul style="list-style-type: none"> Examinar el plan de respuesta ante incidentes (consultar el Requisito 12.10) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿Se llevan a cabo medidas correspondientes cuando se descubren puntos de acceso inalámbricos no autorizados?	<ul style="list-style-type: none"> Entrevistar al personal a cargo Inspeccionar los escaneos inalámbricos recientes y las respuestas relacionadas 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2	<p>¿Se realizan escaneos internos y externos de vulnerabilidades en la red al menos trimestralmente, y después de cada cambio significativo en la red (tales como instalaciones de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos) de la manera siguiente?</p> <p>Nota: Se pueden combinar varios informes de análisis para el proceso de análisis trimestral a fin de demostrar que se analizaron todos los sistemas y que se abordaron todas las vulnerabilidades. Es posible que se solicite documentación adicional para verificar que las vulnerabilidades no resueltas estén en proceso de resolverse.</p> <p>Para el cumplimiento inicial de las PCI DSS, no es necesario tener cuatro análisis trimestrales aprobados si el asesor verifica que 1) el resultado del último análisis fue aprobado, 2) la entidad ha documentado las políticas y los procedimientos que disponen la realización de análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han corregido tal como se muestra en el nuevo análisis. En los años posteriores a la revisión inicial de las PCI DSS, debe haber cuatro análisis trimestrales aprobados.</p>						

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
11.2.1	(a) ¿Se realizan escaneos internos trimestrales de vulnerabilidades?	<ul style="list-style-type: none"> Revisar los informes de escaneo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿El proceso de escaneo interno trimestral incluye nuevos escaneos según requerido hasta que se resuelven todas las vulnerabilidades "de alto riesgo" (de conformidad con lo definido en 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"/>	<input type="checkbox"/>
	(c) ¿Los escaneos internos trimestrales 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"/>	<input type="checkbox"/>
11.2.2	(a) ¿Se realizan escaneos externos trimestrales de vulnerabilidades? 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.	<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"/>	<input type="checkbox"/>
	(b) ¿Los resultados de cada escaneo y repetición de escaneo trimestral satisfacen los requisitos de la Guía del programa ASV para la aprobación de los escaneos? (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"/>	<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"/>	<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	No probado
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? Nota: Los análisis deben estar a cargo de personal calificado.	<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"/>	<input type="checkbox"/>
(b) ¿El proceso de escaneo incluye nuevos análisis hasta que ocurre lo siguiente? <ul style="list-style-type: none"> En el caso de los escaneos externos, no se han registrado vulnerabilidades con puntuaciones CSVV de 4.0 o superior, 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"/>	<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"/>	<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	No probado
11.3 ¿En la metodología de pruebas de penetración se incluye lo siguiente? <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"/>	<input type="checkbox"/>
11.3.1 (a) ¿Se <i>realizan</i> pruebas de penetración externas según la metodología definida al menos una vez al año y después de cualquier modificación significativa de infraestructuras o aplicaciones (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor web al entorno)?	<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"/>	<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? (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"/>	<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	No probado
11.3.2	(a) ¿Se <i>realizan</i> pruebas de penetración internas según la metodología definida al menos una vez al año y después de cualquier modificación significativa de infraestructuras o aplicaciones (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 interna 	<input type="checkbox"/>	<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? (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"/>	<input type="checkbox"/>
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"/>	<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) ¿Estás 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"/>	<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"/>	<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	No probado
(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? (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"/>	<input type="checkbox"/>
11.3.4.1 <i>Solo para proveedores de servicio:</i> Si se utiliza la segmentación: Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.						
(a) ¿Se confirma el alcance de PCI DSS al realizar pruebas de penetración en los controles de segmentación, por lo menos cada seis meses, y después de cualquier cambio a los controles/métodos de segmentación?	<ul style="list-style-type: none"> Examinar los resultados de las pruebas de penetración en los controles de segmentación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Las pruebas de penetración cubren a todos los controles/métodos de segmentación en uso?	<ul style="list-style-type: none"> Examinar los resultados de las pruebas de penetración en los controles de segmentación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) 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 las pruebas de penetración en los controles de segmentación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) ¿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? (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"/>	<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	No probado
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"/>	<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"/>	<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"/>	<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 de 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"/>	<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	No probado
	(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? 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.	<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"/>	<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"/>	<input type="checkbox"/>
11.6	¿Las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad <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"/>	<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	No probado
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"/>	<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"/>	<input type="checkbox"/>
12.2	(a) Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente: <ul style="list-style-type: none"> Identifica activos críticos, amenazas y vulnerabilidades. ¿Da lugar a un análisis formal y documentado del riesgo? <p><i>Los ejemplos de metodologías de evaluación de riesgos incluyen, entre otros, OCTAVE, ISO 27005 y NIST SP 800-30.</i></p>	<ul style="list-style-type: none"> Revisar el proceso de evaluación de riesgos anual Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿El proceso de evaluación de riesgo se realiza, al menos, una vez al año y después de implementar cambios significativos en el entorno (por ejemplo, adquisiciones, fusiones o reubicaciones, etc.)?	<ul style="list-style-type: none"> Revisar la documentación de evaluación de riesgo Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3	¿Hay desarrolladas políticas de uso para las tecnologías críticas que definen cómo usarlas correctamente y que exijan lo siguiente? Nota: Entre los ejemplos de tecnologías críticas, se incluyen las tecnologías inalámbricas y de acceso remoto, las computadoras portátiles, las tabletas, los dispositivos electrónicos extraíbles, el uso del correo electrónico y de Internet.						

Pregunta de las PCI DSS		Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
			Sí	Sí con CCW	No	N/C	No probado
12.3.1	¿Aprobación explícita de las partes autorizadas para utilizar las tecnologías?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	¿Autenticación para el uso de la tecnología?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	¿Una lista de todos los dispositivos y el personal que tenga acceso?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.4	¿Un método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetado, codificación o inventario de dispositivos)?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	¿Usos aceptables de la tecnología?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	¿Ubicaciones aceptables para las tecnologías en la red?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.7	¿Lista de productos aprobados por la empresa?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.8	¿Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.9	¿Activación de las tecnologías de acceso remoto para proveedores y socios de negocio solo cuando sea necesario, con desactivación inmediata después de su uso?	<ul style="list-style-type: none"> ▪ Revisar las políticas de uso ▪ Entrevistar al personal a cargo 	<input type="checkbox"/>	<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	No probado
12.3.10	(a) En el caso del personal que tiene acceso a datos de titulares de tarjetas mediante tecnologías de acceso remoto, ¿prohíbe la política copiar, mover y almacenar los datos de titulares de tarjetas en unidades de disco locales y dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad de negocios definida? <i>Si existe una necesidad comercial autorizada, las políticas de uso deben disponer la protección de los datos de conformidad con los requisitos correspondientes de las PCI DSS.</i>	<ul style="list-style-type: none"> Revisar las políticas de uso Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Para el personal con la autorización correcta, ¿la política exige la protección de los datos de los titulares de tarjetas, de acuerdo con los Requisitos de las PCI DSS?	<ul style="list-style-type: none"> Revisar las políticas de uso Entrevistar al personal a cargo 	<input type="checkbox"/>	<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"/>	<input type="checkbox"/>
12.4.1	<i>Solo para proveedores de servicios: ¿La gerencia ejecutiva ha establecido responsabilidad para la protección de los datos del titular de la tarjeta y de un programa de cumplimiento de PCI DSS, como sigue?: Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.</i>						
	(a) ¿La gerencia ejecutiva ha asignado una responsabilidad general para mantener el cumplimiento de las PCI DSS de la entidad?	<ul style="list-style-type: none"> Examinar documentación 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) ¿La gerencia ejecutiva ha definido una carta para el programa de cumplimiento de las PCI DSS y la comunicación con la gerencia ejecutiva?	<ul style="list-style-type: none"> Examinar carta de las PCI DSS 	<input type="checkbox"/>	<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	No probado
12.5	(a) ¿Se asigna formalmente la seguridad de la información a un Jefe de seguridad u otro miembro de la gerencia relacionado con la seguridad?	<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"/>	<input type="checkbox"/>
	(b) ¿Las siguientes responsabilidades de administración de seguridad de la información están asignadas a una persona o equipo?						
12.5.1	¿Se establecen, documentan y distribuyen políticas y procedimientos de seguridad?	<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"/>	<input type="checkbox"/>
12.5.2	¿Se supervisan y analizan las alertas e información de seguridad, y se distribuyen entre el personal correspondiente?	<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"/>	<input type="checkbox"/>
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"/>	<input type="checkbox"/>
12.5.4	¿Administración de las cuentas de usuario, incluidas las adiciones, eliminaciones y modificaciones?	<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"/>	<input type="checkbox"/>
12.5.5	¿Supervisión y control todo acceso a datos?	<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"/>	<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"/>	<input type="checkbox"/>
	(b) ¿Incluyen los procedimientos de los programas de concienciación sobre seguridad lo siguiente?						

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
12.6.1 (a) ¿El programa de concienciación sobre seguridad proporciona diversos métodos para informar y educar a los empleados sobre la concienciación (por ejemplo, carteles, cartas, notas, capacitación basada en web, reuniones y promociones)? <i>Nota: Los métodos pueden variar según el rol del personal y del nivel de acceso a los datos del titular de la tarjeta.</i>	<ul style="list-style-type: none"> Revisar el programa de concienciación sobre seguridad Revisar los procedimientos del programa de concienciación sobre seguridad Revisar los registros de asistencia del programa de concienciación sobre seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se educa al personal después de la contratación y por lo menos una vez al año?	<ul style="list-style-type: none"> Revisar los procedimientos y la documentación del programa de concienciación sobre seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Los empleados han realizado la capacitación de concienciación y conocen la importancia de la seguridad de los datos del titular de la tarjeta?	<ul style="list-style-type: none"> Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.6.2 ¿Se exige al personal que reconozca al menos una vez al año haber leído y entendido la política y los procedimientos de seguridad de la empresa?	<ul style="list-style-type: none"> Revisar los procedimientos y la documentación del programa de concienciación sobre seguridad 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.7 ¿Se verifican los antecedentes del personal potencial (consulte la definición de “personal” arriba) antes de la contratación a fin de minimizar el riesgo de ataques de fuentes internas? <i>Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias.</i> <i>Nota: En el caso de los posibles candidatos para ser contratados, como cajeros de un comercio, que solo tienen acceso a un número de tarjeta a la vez al realizar una transacción, este requisito es solo una recomendación.</i>	<ul style="list-style-type: none"> Entrevistar a la gerencia del departamento de Recursos Humanos 	<input type="checkbox"/>	<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	No probado
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"/>	<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"/>	<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"/>	<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"/>	<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	No probado
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"/>	<input type="checkbox"/>
12.9	<p><i>Solo para proveedores de servicios: ¿Los proveedores de servicios aceptan, por escrito y ante los clientes, 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?</i></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"> Revisar las políticas y los procedimientos del proveedor de servicios Observar las plantillas de los acuerdos escritos 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10	¿Se ha implementado un plan de respuesta a incidentes como preparación para reaccionar inmediatamente a un fallo del sistema, de la siguiente manera?						
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"/>	<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"/>	<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"/>	<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	No probado
	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>
12.10.2	¿Se revisa y se prueba el plan, por lo menos anualmente, incluidos todos los elementos enumerados en el Requisito 12.10.1?	<ul style="list-style-type: none"> Revisar los procesos del plan de respuesta a incidentes Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.3	¿Se ha designado personal especializado que se encuentre disponible permanentemente para responder a las alertas?	<ul style="list-style-type: none"> Observar los procesos Revisar las políticas Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.4	¿Se proporciona capacitación adecuada al personal sobre las responsabilidades de respuesta ante fallos de seguridad?	<ul style="list-style-type: none"> Observar los procesos Revisar los procesos del plan de respuesta a incidentes Entrevistar al personal a cargo 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.5	¿Se incluyen las alertas de los sistemas de supervisión de seguridad en el plan de respuesta a incidentes?	<ul style="list-style-type: none"> Observar los procesos Revisar los procesos del plan de respuesta a incidentes 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.6	¿Se ha elaborado un proceso para modificar y desarrollar el plan de respuesta a incidentes según las lecciones aprendidas, e incorporar los desarrollos de la industria?	<ul style="list-style-type: none"> Observar los procesos Revisar los procesos del plan de respuesta a incidentes Entrevistar al personal a cargo 	<input type="checkbox"/>	<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	No probado
<p>12.11 <i>Solo para proveedores de servicio: ¿Se realizan revisiones, por lo menos trimestralmente, para confirmar que el personal está siguiendo las políticas y los procedimientos operativos de seguridad, como sigue?:</i></p> <p>Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.</p>						
<p>(a) ¿Las revisiones cubren los siguientes procesos?:</p> <ul style="list-style-type: none"> • Revisiones de registros diarios • Revisiones de conjunto de reglas de Firewall • Aplicar normas de configuración a los nuevos sistemas • Responder a las alertas de seguridad • Cambiar los procesos de gestión 	<ul style="list-style-type: none"> ▪ Examinar las políticas y los procedimientos para realizar las revisiones trimestrales ▪ Entrevistar al personal 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>(b) ¿Se realizan las revisiones, por lo menos trimestralmente?</p>	<ul style="list-style-type: none"> ▪ Entrevistar al personal ▪ Examinar registros de revisiones 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>12.11.1 <i>Solo para proveedores de servicio: ¿Se mantiene la documentación del proceso de revisión trimestral para incluir?:</i></p> <ul style="list-style-type: none"> • Documentar los resultados de las revisiones • Revisar y cerrar los resultados por parte del personal asignado para asumir la responsabilidad del programa de cumplimiento de las PCI DSS <p>Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.</p>	<ul style="list-style-type: none"> ▪ Examinar la documentación de las revisiones trimestrales 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Anexo A: Requisitos adicionales de las PCI DSS

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

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)				
		Sí	Sí con CCW	No	N/C	No probado
<p>A1 ¿Se protege el entorno y los datos alojados de cada entidad (es decir comerciante, proveedor de servicios u otra entidad), según A.1.1 a A.1.4 de la siguiente manera?:</p> <p><i>Un proveedor de hosting debe cumplir con estos requisitos, así como también con las demás secciones correspondientes de PCI DSS.</i></p> <p>Nota: Aunque posiblemente el proveedor de hosting cumpla con estos requisitos, no se garantiza el cumplimiento de la entidad que utiliza al proveedor de hosting. Cada entidad debe cumplir con las PCI DSS y validar el cumplimiento, según corresponda.</p>						
<p>A1.1 ¿Realiza cada entidad procesos con acceso al entorno de datos de titulares de tarjetas de la entidad, y los procesos de esta aplicación se ejecutan utilizando la ID única de la entidad?</p> <p><i>Por ejemplo:</i></p> <ul style="list-style-type: none"> Ninguna entidad del sistema puede utilizar una ID de usuario de servidor Web compartida. Todas las secuencias de comandos CGI utilizadas por una entidad se deben crear y ejecutar como ID de usuario única de la entidad. 	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y las identificaciones exclusivas relacionadas para las entidades en el hosting 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>A1.2 ¿Se encuentran los privilegios y accesos de cada entidad restringidos a su propio entorno de datos de titulares de tarjetas de la siguiente manera?</p> <p>(a) ¿No son las ID de usuario de cualquier proceso de aplicación un usuario con privilegios (raíz/admin)?</p>	<ul style="list-style-type: none"> Examinar las configuraciones del sistema en función de las ID de usuario de la aplicación 	<input type="checkbox"/>	<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	No probado
(b) ¿Ha leído, escrito o ejecutado cada entidad permisos solo para los archivos y directorios que tiene o para los archivos necesarios para el sistema (restringidos mediante permisos de sistema de archivos, listas de control de acceso, chroot, jailshell, etc.)? Importante: Los archivos de una entidad no deben compartirse de forma grupal.	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y los permisos de archivo para las entidades en el hosting 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Ninguno de los usuarios de una entidad tiene acceso de escritura a archivos binarios compartidos del sistema?	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y los permisos de archivo para los archivos binarios del sistema 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) ¿Se restringe la visualización de las entradas del registro a la entidad propietaria?	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y los permisos de archivo para ver las entradas del registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) ¿Se han implementado restricciones para el uso de estos recursos del sistema? <ul style="list-style-type: none"> Espacio en disco, Ancho de banda, Memoria, CPU Esto asegura que ninguna entidad pueda acaparar los recursos del servidor y aprovecharse de las vulnerabilidades (por ejemplo, error, carrera y condiciones de reinicio que tienen como resultado, por ejemplo, desbordamientos de buffer).	<ul style="list-style-type: none"> Examinar las configuraciones del sistema y los permisos de archivo para el uso de: <ul style="list-style-type: none"> Espacio en disco Ancho de banda Memoria CPU 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A1.3 (a) ¿Se han habilitado registros y pistas de auditoría y son exclusivos para el entorno de datos de titulares de tarjetas de cada entidad, en concordancia con el Requisito 10 de las PCI DSS?	<ul style="list-style-type: none"> Examinar los parámetros del registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) ¿Se han habilitado registros de la siguiente manera para cada comerciante y entorno de proveedor de servicios?						

Pregunta de las PCI DSS	Pruebas esperadas	Respuesta (Marque únicamente una respuesta para cada pregunta)					
		Sí	Sí con CCW	No	N/C	No probado	
<ul style="list-style-type: none"> ¿Se habilitan los registros para aplicaciones comunes de tercero? 	<ul style="list-style-type: none"> Examinar los parámetros del registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<ul style="list-style-type: none"> ¿Están activos los registros de forma predeterminada? 	<ul style="list-style-type: none"> Examinar los parámetros del registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<ul style="list-style-type: none"> ¿Están disponibles los registros para la revisión de la entidad propietaria? 	<ul style="list-style-type: none"> Examinar los parámetros del registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<ul style="list-style-type: none"> ¿Se comunica la ubicación de los registros con claridad a la entidad propietaria? 	<ul style="list-style-type: none"> Examinar los parámetros del registro 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A1.4	<ul style="list-style-type: none"> ¿Se han habilitado los procesos para proporcionar una investigación forense oportuna en caso de riesgos para un comerciante o proveedor de servicios alojado? 	<ul style="list-style-type: none"> Revisar las políticas y los procedimientos escritos 	<input type="checkbox"/>				

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	No probado
<p>A2.1 <i>Para los terminales POS POI (y los puntos de terminación SSL/TLS a los que se conectan) utilizando SSL y/o TLS temprana:</i></p> <ul style="list-style-type: none"> Se confirmaron los dispositivos para que no sean susceptibles a ninguna explotación conocida para SSL/TLS temprana O: ¿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 verifica los dispositivos POS POI que no son susceptibles a ninguna explotación conocida para SSL/TLS temprana 	<input type="checkbox"/>	<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	No probado
<p>A2.2 Hay un Plan de migración y de Mitigación de riesgo formal implementado para todas las implementaciones que usan SSL y/o TLS temprana (que no sea lo permitido en el Requisito A2.1), que incluya:</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 para supervisar 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"/>	<input type="checkbox"/>
<p>A2.3 <i>Solo para proveedores de servicio:</i> ¿Hay una oferta de servicio seguro implementada?</p> <p>Nota: Antes del 30 de junio de 2016, el proveedor de servicios debe tener una opción de protocolo seguro incluida en su oferta de servicio, o tener un Plan de migración y de Mitigación de riesgo documentado (según A2.2) que incluya una fecha límite para proporcionar una opción de protocolo seguro, no más allá del 30 de junio de 2016. Después de esta fecha, todos los proveedores de servicios deben ofrecer una opción de protocolo seguro para su servicio.</p>	<ul style="list-style-type: none"> ▪ Examinar las configuraciones del sistema y la documentación de apoyo 	<input type="checkbox"/>	<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(s) de pago o por un adquirente que requieren una validación adicional de los requisitos de las 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: Solo 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 D (Sección 2), con fecha (*fecha de finalización del SAQ*).

Según los resultados observados en el SAQ D 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 las 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 proveedor de servicios</i>) ha demostrado un cumplimiento total con las PCI DSS.</p>						
<input type="checkbox"/>	<p>Falta de cumplimiento: No se han completado todas las secciones del SAQ de las PCI DSS o se ha respondido en forma negativa a algunas de las preguntas, lo que resulta en una calificación general de FALTA DE CUMPLIMIENTO, y (<i>nombre de la empresa del proveedor de servicios</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 las marcas 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: 30%; text-align: center;">Requisito afectado</th> <th style="text-align: center;">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 D de las PCI DSS, Versión (<i>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, datos de CAV2, CVC2, CID, o CVV2 ¹ , ni datos de PIN ² después de encontrarse la autorización de la transacción en NINGÚN sistema revisado durante la presente evaluación. ³
<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. Atestación del proveedor de servicios

<i>Firma del Oficial Ejecutivo del proveedor de servicios</i> ↑	<i>Fecha:</i>
<i>Nombre del Oficial Ejecutivo del proveedor de servicios:</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:	
--	--

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

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.

empresa espera cumplir con el requisito y una breve descripción de las medidas que se tomarán para cumplirlo.
Consulte con las marcas de pago correspondientes 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	Instalar y mantener 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	Proteger los datos almacenados del titular de la tarjeta.	<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 de 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 los accesos a los recursos de red y a los datos de los titulares de las tarjetas	<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 A1	Requisitos adicionales de las PCI DSS para proveedores de hosting compartido	<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"/>	

