# Payment Card Industry
# Estándar de Seguridad de Datos

## Cuestionario de Autoevaluación D para Comerciantes y Certificado de Conformidad

### Para uso con el PCI DSS Versión 4.0.1

Fecha de Publicación: Octubre de 2024

*DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerarse, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.*

# Cambios en el Documento

| Fecha | Versión PCI DSS | Revisión SAQ | Descripción |
|---|---|---|---|
| Octubre de 2008 | 1.2 | | Para alinear el contenido con el nuevo estándar PCI DSS v1.2 e implementar los cambios menores observados desde la v1.1 original. |
| Octubre de 2010 | 2.0 | | Para alinear el contenido con los nuevos 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 PCI DSS v3.0 e incorporar opciones de respuesta adicionales. |
| Abril de 2015 | 3.1 | | Actualizado para alinearse con PCI DSS v3.1. Para ver los detalles de cambios en PCI ver *PCI DSS –Resumen de Cambios de la Versión PCI DSS 3.0 a 3.1.* |
| Julio de 2015 | 3.1 | 1.1 | Actualizado para eliminar las referencias a las "mejores prácticas" previas al 30 de junio de 2015 y para eliminar la opción de notificación PCI DSS v2 para el requisito 11.3 |
| Abril de 2016 | 3.2 | 1.0 | Actualizado para alinearse con PCI DSS v3.2. Para ver los detalles de cambios en PCI ver PCI DSS –*Resumen de Cambios de la Versión PCI DSS 3.1 a 3.2.* |
| Enero de 2017 | 3.2 | 1.1 | Se actualizó la numeración de la versión para alinearla con otros SAQ. |
| Junio de 2018 | 3.2.1 | 1.0 | Actualizado para alinearse con PCI DSS v3.2.1. Para ver los detalles de cambios en PCI ver PCI DSS –*Resumen de Cambios de la Versión PCI DSS 3.2 a 3.2.1.* |
| Abril de 2022 | 4.0 | | Actualizado para alinearse con PCI DSS v4.0. Para ver los detalles de cambios en PCI ver PCI DSS –Resumen de Cambios de la Versión PCI DSS 3.2.1 a 4.0.<br>Se ha reordenado, re-titulado y ampliado la información de la sección "Cómo Llenar el Cuestionario de Autoevaluación" (previamente titulada "Antes de Empezar").<br>Alineación del contenido de las Secciones 1 y 3 del Certificado de Conformidad (AOC) con el Informe de Conformidad AOC PCI DSS v4.0.<br>Se agregaron los Requisitos de PCI DSS v4.0<br>Se agregaron anexos como apoyo para nuevas respuestas a notificaciones. |

| | | | |
|---|---|---|---|
| Diciembre de 2022 | 4.0 | 1 | Se ha eliminado "Implementado con Remediación" como opción de informe de la tabla de Respuestas a los Requisitos, de la Parte 2g del Certificado de Conformidad (AOC), de la columna de Respuestas de la Sección 2 del SAQ y de la Sección 3 del AOC.<br>También se ha eliminado el antiguo Anexo C.<br>Se agregó "Implementado con CCW" a la Sección 3 de AOC.<br>Se agregó la orientación para responder a los requisitos con fecha futura.<br>Se agregaron aclaraciones menores y se corrigieron errores tipográficos. |
| Octubre de 2024 | 4.0.1 | | Actualizado para alinearse con PCI DSS v4.0.1. Para ver los detalles de cambios en *PCI ver PCI DSS –Resumen de Cambios de la Versión PCI DSS 4.0 a 4.0.1.*<br>Se agregó la Guía de Recursos ASV a la sección “Recursos Adicionales PCI SSC.” |

# Contenido

# Llenando el Cuestionario de Autoevaluación

## Criterios de Elegibilidad del Comerciante para el Cuestionario de Autoevaluación D

El Cuestionario de Autoevaluación (SAQ) D para Comerciantes se aplica a los comerciantes que reúnen los requisitos para rellenar un cuestionario de autoevaluación pero que no cumplen con los criterios de ningún otro tipo de SAQ. Algunos ejemplos de entornos de comerciantes a los que puede aplicarse el SAQ D son, entre otros, los siguientes:

- Comerciantes de comercio electrónico que aceptan datos del titular de la tarjeta en su sitio web.
- Comerciantes que almacenan electrónicamente los datos del titular de la tarjeta.
- Comerciantes que no almacenan datos del titular de la tarjeta electrónicamente pero que no cumplen con los criterios de otro tipo de SAQ.
- Comerciantes con entornos que podrían cumplir los criterios de otro tipo de SAQ, pero que tienen requisitos adicionales PCI DSS aplicables a su entorno.

***Este SAQ no aplica para los proveedores de servicios.***

## Definición de Datos del Titular de la Tarjeta, Datos de Tarjetahabiente y Datos de Autenticación Sensibles

Los PCI DSS está destinado a todas las entidades que almacenan, procesan o transmiten datos de tarjetahabiente (CHD) y/o datos de autenticación sensibles (SAD) o que podrían afectar la seguridad de los datos del tarjetahabiente y/o sus datos de autenticación sensibles. Los datos de tarjetahabiente y los datos de autenticación sensibles se consideran datos del titular de la tarjeta y se definen de la siguiente manera:

| Datos del Titular de la Tarjeta | |
|---|---|
| **Los Datos de Tarjetahabiente incluyen:** | **Los Datos de Autenticación Sensibles incluyen:** |
| • Número de cuenta principal (PAN)<br>• Nombre del Tarjetahabiente<br>• Fecha de Expiración<br>• Código de servicio | • Datos de pista completos (datos de banda magnética o equivalentes en un chip)<br>• Código de Verificación de la Tarjeta<br>• PINs / Bloques de PIN |

Refiérase a la Sección 2 PCI DSS, *Información de Aplicabilidad PCI DSS,* para más detalles.

## Pasos para Completar la Autoevaluación PCI DSS

1. Confirme mediante la revisión de los criterios de elegibilidad en este SAQ y en el documento *Instrucciones y Directrices del Cuestionario de Autoevaluación* en el sitio web de PCI SSC que éste es el SAQ correcto para el entorno del comerciante.
2. Confirme que el entorno del comerciante está correctamente enfocado.
3. Evalúe el entorno para comprobar la conformidad con los requisitos de PCI DSS.
4. Llene todas las secciones de este documento:
   - Sección 1: Información de la Evaluación (partes 1 & 2 de la Declaración de Conformidad (AOC): Información de Contacto y Resumen Ejecutivo.
   - Sección 2: Cuestionario de Autoevaluación D para Comerciantes.
   - Sección 3: Detalles de Validación y Certificación (Partes 3 & 4 de la AOC - Validación PCI DSS y Plan de Acción para Requisitos de No-Conformidad (si aplica la Parte 4)).
5. Presente el SAQ y el AOC, junto con cualquier otra documentación solicitada -tal como los informes ASV escaneados- a la organización solicitante (aquellas organizaciones que gestionan los programas de conformidad, como las marcas de pago y los adquirentes).

## Pruebas Previstas

Las instrucciones que aparecen en la columna "Pruebas Previstas" se basan en los procedimientos de prueba PCI DSS y brindan una descripción de alto nivel de los tipos de actividades de prueba que se esperan que un comerciante desarrolle para verificar que se ha cumplido con un requisito.

La intención detrás cada método de prueba se describe como sigue:

- Evalúe: El comerciante evalúa críticamente las evidencias de datos. Algunos ejemplos comunes incluyen documentos (electrónicos o físicos), capturas de pantalla, archivos de configuración, registros de auditoría y archivos de datos.
- Observe: El comerciante observa una acción o percibe algo en el entorno. Algunos ejemplos de sujetos de observación incluyen el desempeño del personal en una tarea o un proceso, los componentes del sistema que realizan una función o responden a una entrada, las condiciones del entorno y los controles físicos.
- Entreviste: El comerciante conversa con el personal de manera individual. Los objetivos de la entrevista pueden incluir la confirmación de si se realiza una actividad, las descripciones de cómo se realiza una actividad y si el personal tiene conocimientos o comprensión particulares.

Los métodos de prueba de prueba tienen por objeto permitir al comerciante demostrar cómo ha cumplido un requisito. Los elementos específicos que deben evaluarse u observarse y el personal que será entrevistado deben ser apropiados tanto para el requisito que se está evaluando como para la implementación particular de la entidad.

Los detalles completos de los procedimientos de prueba para cada requisito pueden encontrarse en PCI DSS.

## Respuestas a los Requisitos

Para cada elemento del requisito hay una opción de respuestas para indicar la situación del comerciante con respecto a ese requisito. ***Sólo debe seleccionarse una respuesta para cada elemento del requisito.***

En la tabla siguiente se describe el significado de cada respuesta:

| Respuesta | Cuándo utilizar esta respuesta: |
|---|---|
| **Implementado** | Se han realizado las pruebas previstas y se ha cumplido con todos los elementos del requisito según lo establecido. |
| **Implementado con CCW**<br>(Hoja de Control Compensatorio) | Se han realizado las pruebas previstas y se ha cumplido con el requisito con la ayuda de un control compensatorio.<br>Todas las respuestas en esta columna requieren que se llene la Hoja de Control Compensatorio (CCW) que aparece en el Anexo B de este SAQ.<br>En los Anexos B y C de PCI DSS se proporciona información sobre el uso de controles compensatorios y orientación sobre cómo llenar la hoja de trabajo. |
| **No Aplicable** | Este requisito no aplica al entorno del comerciante. (Refiérase a "Orientación sobre los Requisitos No Aplicables" a continuación).<br>Todas las respuestas en esta columna requieren una explicación de respaldo en el Anexo C de este SAQ. |
| **No Probado** | El requisito no se incluyó para su consideración en la evaluación y no se sometió a una prueba de ninguna manera. (Véase "Comprender la diferencia entre No Aplicable y Probado" más adelante para acceder a ejemplos de cuándo debe utilizarse esta opción).<br>Todas las respuestas de esta columna requieren una explicación de respaldo en el Anexo D de este SAQ. |
| **No Implementado** | Algunos o todos los elementos del requisito no se han cumplido, o están en proceso de implementación, o requieren más pruebas antes de que el comerciante pueda confirmar que han sido implementados. Las respuestas de esta columna pueden requerir la ejecución de la Parte 4 si así lo solicita la entidad a la que se presentará este SAQ.<br>Esta respuesta también se utiliza si un requisito no puede cumplirse debido a una restricción legal. (Para más orientación refiérase a "Excepción legal" más adelante). |

### *Orientación sobre los Requisitos No Aplicable*

Aunque muchos comerciantes que llenen el SAQ D necesitarán validar la conformidad de todos los requisitos de PCI DSS, algunas entidades con modelos de negocio muy específicos pueden encontrar que algunos requisitos no les son aplicables. Por ejemplo, las entidades que no utilizan la tecnología inalámbrica de ninguna manera, no se espera que cumplan con los Requisitos de PCI DSS que son específicos para la gestión de la tecnología inalámbrica. Igualmente, no se espera que las entidades que no almacenan ningún dato del titular de la tarjeta electrónicamente en ningún momento, cumplan con los requisitos de PCI DSS relacionados con el almacenamiento seguro de los datos del titular de la tarjeta (por ejemplo, el requisito 3.5.1). Otro ejemplo son los requisitos específicos para el desarrollo de aplicaciones y la codificación segura (por ejemplo, los requisitos 6.2.1 a 6.2.4), que sólo se aplican a una entidad con software a medida (desarrollado para la entidad por un tercero según las especificaciones de la entidad) o software personalizado (desarrollado por la entidad para su propio uso).

Para cada respuesta en la que se seleccione No Aplicable en este SAQ, llene el Anexo C: Explicación de los Requisitos Señalados como No Aplicable.

### *Comprender la diferencia entre No Aplicable y No Probado*

Los requisitos que se consideran no aplicables a un entorno deben verificarse como tales. Utilizando el ejemplo inalámbrico anterior, para que un comerciante seleccione "No Aplicable" para los requisitos 1.3.3, 2.3.1, 2.3.2 y 4.2.1.2, el comerciante debe confirmar primero que no se utilizan tecnologías inalámbricas en su entorno de datos de tarjetahabiente (CDE) o que se conectan a su CDE. Una vez confirmado esto, el comerciante puede seleccionar "No Aplicable" para esos requisitos específicos.

Si un requisito se excluye completamente de la revisión sin tener en cuenta si *podría aplicarse,* deberá seleccionarse la opción "No Probado". Algunos ejemplos de situaciones en las que esto podría ocurrir son:

- Un adquiriente solicita a un comerciante que valide un subconjunto de requisitos, por ejemplo, utilizando el Enfoque Prioritario PCI DSS para validar sólo determinados hitos.
- Un comerciante está confirmando un nuevo control de seguridad que afecta sólo a un subconjunto de requisitos, por ejemplo, la implementación de una nueva metodología de cifrado que sólo requiere la evaluación de los requisitos 2, 3 y 4 de PCI DSS.

En ese tipo de escenarios, la evaluación del comerciante sólo incluye algunos Requisitos de PCI DSS aunque se pueden aplicar otros requisitos a su entorno.

Si algún requisito está completamente excluido de la autoevaluación del comerciante, seleccione No Probado para ese requisito específico y llene el Anexo D: Explicación de los Requisitos no Probados para cada entrada "No Probado". Una evaluación con cualquier respuesta "No Probado" se considera una evaluación PCI DSS "Parcial" y el comerciante la anotará como tal en la Declaración de Conformidad de la Sección 3, Parte 3 de este SAQ.

### *Orientación para Responder a Requisitos con Fecha Futura*

En la Sección 2 a continuación, cada requisito o punto PCI DSS con un período de implementación extendido incluye la siguiente nota: *"Este requisito [o punto] es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*"

No se requiere que estos nuevos requisitos se incluyan en una evaluación PCI DSS hasta que haya pasado esa fecha futura. Antes de esa fecha futura, cualquier requisito con una fecha de implementación extendida que no haya sido implementado por el comerciante puede marcarse como

No Aplicable y documentarse en el *Anexo C: Explicación de los Requisitos Señalados como No Aplicable.*

### *Excepción Legal*

Si su organización está sujeta a una restricción legal que le impide cumplir con un Requisito de PCI DSS, seleccione No Implementado para ese requisito y llene la declaración correspondiente en la Sección 3, Parte 3 de este SAQ.

***Nota:*** *Una excepción legal es una restricción legal debido a una ley, regulación o requisito regulatorio local o regional, donde cumplir con un requisito del PCI DSS violaría esa ley, regulación o requisito regulatorio. Las obligaciones contractuales o el asesoramiento legal no son restricciones legales.*

*Las obligaciones contractuales o el asesoramiento legal no son restricciones legales.*

### *Uso del Enfoque Personalizado*

Los SAQ no pueden utilizarse para documentar el uso del Enfoque Personalizado para cumplir con los Requisitos de PCI DSS. Por esta razón, los Objetivos del Enfoque Personalizado no se incluyen en los SAQ. Las entidades que deseen validar el uso del Enfoque Personalizado pueden utilizar la Plantilla de Informe de Conformidad (ROC) PCI DSS para documentar los resultados de su evaluación.

*El uso del Enfoque Personalizado no está contemplado en los SAQ.*

El uso del enfoque personalizado puede ser regulado por las organizaciones que administran los programas de conformidad, como las marcas de pago y los adquirentes. Las preguntas sobre el uso de un enfoque personalizado deben remitirse a esas organizaciones. Esto incluye si una entidad que es elegible para un SAQ puede, en cambio, completar un ROC para usar un enfoque personalizado, y si se requiere que una entidad utilice QSA, o puede usar un ISA, para completar una evaluación utilizando el enfoque personalizado. La información acerca del uso del Enfoque Personalizado puede encontrarse en los Anexos D y E de PCI DSS.

## Recursos Adicionales PCI SSC

A continuación, se ofrecen recursos adicionales PCI DSS que brindan orientación sobre sus requisitos y sobre cómo llenar el cuestionario de autoevaluación para asistir en el proceso de evaluación.

| Recurso | Incluye: |
|---|---|
| Requisitos y Procedimientos de Prueba del Estándar de Seguridad de Datos PCI (PCI DSS) | ▪ Orientación sobre el Alcance<br>▪ Orientación sobre el objetivo de todos los Requisitos de PCI DSS<br>▪ Detalles de los Procedimientos de Prueba<br>▪ Guía de los Controles Compensatorios<br>▪ Anexo G: Glosario de Términos, Abreviaturas y Acrónimos |
| Instrucciones y Directrices SAQ | ▪ Información sobre todos los SAQ y sus Criterios de Elegibilidad<br>▪ Cómo determinar qué SAQ es el adecuado para su organización |
| Preguntas frecuentes (FAQ) | ▪ Orientación e Información acerca de los SAQ. |
| Glosario PCI DSS en línea | ▪ Términos, Abreviaturas y Acrónimos PCI DSS |
| Información Complementaria y Directrices | ▪ Directrices en varios temas PCI DSS incluyendo:<br>– *Comprendiendo el Alcance PCI DSS y la Segmentación de la Red*<br>– *Garantía de Seguridad de Terceros*<br>– *Orientación sobre la Autenticación Multifactorial*<br>– *Mejores Prácticas para Mantener la Conformidad con PCI DSS* |
| Introducción a PCI | ▪ Recursos para pequeños comerciantes, incluyendo:<br>– *Guía de Pagos Seguros*<br>– *Sistemas de Pago Comunes*<br>– *Preguntas que hacer a sus Proveedores*<br>– *Glosario de Términos de Seguridad de Pagos e Información*<br>– *Conceptos Básicos PCI Firewall*<br>– *Guía de Recursos ASV* |

Estos y otros recursos pueden encontrarse en el sitio web de PCI SSC (www.pcisecuritystandards.org).

Se aconseja a las organizaciones que revisen los documentos PCI DSS y otros documentos de respaldo antes de comenzar una evaluación.

# Sección 1: Información de la Evaluación

### *Instrucciones para la Presentación*

Este documento debe ser completado como una declaración de los resultados de la autoevaluación del comerciante con respecto a los *Requisitos y Procedimientos de Prueba del Estándar de Seguridad de Datos de Payment Card Industry (PCI DSS)* Complete todas las secciones. El comerciante es responsable de garantizar que cada sección sea completada por las partes pertinentes, según corresponda. Póngase en contacto con la(s) entidad(es) que recibirán el AOC para los procedimientos de elaboración de informe y presentación.

## Parte 1. Información de Contacto

**Parte 1a. Comerciante Evaluado**

| | |
|---|---|
| Nombre de la compañía: | |
| DBA (actuando comercialmente como): | |
| Dirección postal de la compañía: | |
| Sitio web principal de la compañía: | |
| Nombre del contacto de la compañía: | |
| Título del contacto de la compañía: | |
| Número de teléfono del contacto: | |
| Dirección de correo electrónico del contacto: | |

**Parte 1b. Asesor**

Provea la siguiente información sobre todos los asesores que participaron en la evaluación. Si no hubo ningún asesor para un tipo de asesor determinado, introduzca No aplicable.

| | |
|---|---|
| Asesor(es) de Seguridad Interna PCI SSC | |
| Nombre del ISA: | |
| Asesor de Seguridad Calificado | |
| Nombre de la compañía: | |
| Dirección postal de la compañía: | |
| Página web de la compañía: | |
| Nombre del Asesor principal: | |
| Número de teléfono del asesor: | |
| Dirección de correo electrónico del asesor: | |
| Número de certificado del asesor: | |

## Parte 2. Resumen Ejecutivo

### Parte 2a. Canales de Pago del Comerciante (seleccione todos los que apliquen):

Indique todos los canales de pago utilizados por la empresa que se incluyen en esta Evaluación.

☐ Pedido por correo / por teléfono (MOTO)

☐ Comercio electrónico

☐ Presencial

| | |
|---|---|
| ¿Hay algún canal de pago que no esté incluido en esta evaluación?<br>En caso afirmativo, indique qué canal(les) no están incluidos en la evaluación y explique brevemente por qué se han excluido. | ☐ Sí ☐ No |

***Nota:*** *Si el comerciante tiene un canal de pago no cubierto por esta SAQ, consulte con la(s) entidad(es) a la(s) que se presentará esta AOC acerca de la validación para los otros canales.*

### Parte 2b. Descripción de la Función con Tarjetas de Pago

Para cada canal de pago incluido en esta Evaluación seleccionado en la Parte 2a previa, describa cómo la empresa almacena, procesa y/o transmite los datos del titular de la tarjeta.

| **Canal** | **Cómo la Empresa Almacena, Procesa y/o Transmite los Datos del Titular de la Tarjeta** |
|---|---|
| | |
| | |
| | |

### Parte 2c. Descripción del Entorno de las Tarjetas de Pago

| | |
|---|---|
| Proporcione una descripción de ***alto- nivel*** del entorno cubierto por esta Evaluación.<br>*Por ejemplo:*<br>• *Conexiones desde y hacia el entorno de datos de tarjetahabiente (CDE).*<br>• *Componentes críticos del sistema dentro del CDE, tales como dispositivos POI, bases de datos, servidores web, etc., y cualquier otro componente de pago necesario, según corresponda.*<br>• *Componentes del sistema que podrían afectar la seguridad de los datos del titular de la tarjeta.* | |
| Indique si el entorno incluye la segmentación para reducir el alcance de la evaluación.<br>*(Consulte la sección "Segmentación" de PCI DSS para obtener orientación sobre la segmentación).* | ☐ Sí ☐ No |

## Parte 2. Resumen Ejecutivo *(continuación)*

### Parte 2d. Localidades e Instalaciones en el Ámbito de Aplicación

Enumere todos los tipos de ubicaciones físicas/instalaciones (por ejemplo, establecimientos minoristas, oficinas corporativas, centros de datos, centros de llamadas y salas de correo) en el ámbito de la evaluación PCI DSS.

| **Tipo de Instalación** | **Número total de Instalaciones** (Cuántas instalaciones de este tipo se encuentran dentro del ámbito) | **Ubicación(ones) de las Instalaciones (ciudad, país)** |
|---|---|---|
| *Ejemplo: Centros de Datos* | *3* | *Boston, MA, USA* |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

### Parte 2e. Productos y Soluciones Validados por PCI SSC

¿Utiliza el comerciante algún elemento identificado en alguna de las listas de Productos y Soluciones Validados por PCI SSC♦?

☐ Sí ☐ No

Provea la siguiente información sobre cada elemento que el comerciante utiliza de las Listas de Productos y Soluciones Validados por PCI SSC.

| **Nombre del Producto o Solución validado por PCI SSC** | **Versión del Producto o Solución** | **Estándar PCI SSC según el cual se validó el producto o la solución** | **Número de Referencia de la Lista PCI SSC** | **Fecha de Expiración de la Lista** (DD-MM-AAAA) |
|---|---|---|---|---|
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |
| | | | | DD-MM-AAAA |

♦ Para los fines de este documento, se entenderá por "Listas de Productos y Soluciones Validados" las listas de productos, soluciones y/o componentes validados que aparecen en el sitio web de PCI SSC (www.pcisecuritystandards.org) por ejemplo, los Kits de Desarrollo de Software 3DS, los Dispositivos PTS Aprobados, el Software de Pago Validado, las Soluciones Cifradas de Punto a Punto (P2PE), las Soluciones de Introducción de PIN basadas en software en COTS (SPoC), las Soluciones de Pago sin contacto en COTS (CPoC) y los Productos de Métodos de Pagos Móviles en COTS (MPoC).

## Parte 2. Resumen Ejecutivo *(continuación)*

### Parte 2f. Proveedores de Servicios Externos

Tiene el comerciante relaciones con uno o más proveedores de servicios externos que:

| | |
|---|---|
| • Almacenan, procesan o transmiten datos del titular de la tarjeta en nombre del comerciante (por ejemplo, pasarelas de pago, procesadores de pago, proveedores de servicios de pago (PSP) y almacenamiento externo). | ☐ Sí ☐ No |
| • Gestionan los componentes del sistema incluidos en el ámbito de la evaluación PCI DSS del comerciante, por ejemplo, a través de servicios de control de seguridad de la red, servicios antimalware, gestión de eventos e incidentes de seguridad (SIEM), centros de contacto y de llamadas, servicios de alojamiento web y proveedores de IaaS, PaaS, SaaS y FaaS en la nube. | ☐ Sí ☐ No |
| • Podrían afectar la seguridad del CDE del comerciante (por ejemplo, proveedores que prestan asistencia a través de acceso remoto, y/o desarrolladores de software a la medida). | ☐ Sí ☐ No |

***En caso afirmativo:***

| **Nombre del proveedor de servicio:** | **Descripción del servicio(s) prestado(s):** |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

***Nota:*** *El Requisito 12.8 aplica a todas las entidades que aparecen en la lista.*

## Parte 2. Resumen Ejecutivo *(continuación)*

### Parte 2g. Resumen de la Evaluación

*(Sección 2 del SAQ y anexos relacionados)*

*Indique a continuación todas las respuestas seleccionadas para cada Requisito de PCI DSS.*

| Requisito de PCI DSS | Respuestas a los Requisitos<br>*Se puede seleccionar más de una respuesta para un requisito determinado. Indique todas las respuestas que correspondan.* | | | | |
|---|---|---|---|---|---|
| | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| Requisito 1: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 2: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 3: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 4: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 5: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 6: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 7: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 8: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 9: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 10: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 11: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requisito 12: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Anexo A2: | ☐ | ☐ | ☐ | ☐ | ☐ |

# Sección 2: Cuestionario de Autoevaluación D para Comerciantes

***Nota:*** *Los siguientes requisitos son un reflejo de los requisitos del documento de Requisitos y Procedimientos de Prueba PCI DSS.*

**Fecha de finalización de la autoevaluación:** DD-MM-AAAA

## Construir y Mantener una Red y Sistemas Segura

### *Requisito 1: Instalar y Mantener los Controles de Seguridad de la Red*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **1.1** Se definen y comprenden los procesos y mecanismos para instalar y mantener los controles de seguridad de la red. | | | | | | | |
| **1.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 1 son:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 1 están documentadas, asignadas y comprendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2** Se configuran y mantienen los controles de seguridad de la red (NSC). | | | | | | | |
| **1.2.1** | Los estándares de configuración para el conjunto de reglas de los NSC son:<br>• Definidos.<br>• Implementados.<br>• Mantenidos. | • Evalúe los estándares de configuración.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **1.2.2** | Todos los cambios en las conexiones de red y en las configuraciones de los NSC se aprueban y gestionan de acuerdo con el proceso de control de cambios definido en el Requisito 6.5.1. | • Evalúe los procedimientos documentados.<br>• Evalúe las configuraciones de redes.<br>• Evalúe los registros de control de cambios.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad** | | | | | | |
| | Los cambios en las conexiones de red incluyen la adición, eliminación o modificación de una conexión.<br>Los cambios en las configuraciones del NSC incluyen aquellos relacionados con el propio componente, así como los que afectan la forma en que realiza su función de seguridad. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **1.2.3** | Se mantienen diagramas de red precisos que muestran todas las conexiones entre el CDE y otras redes, incluyendo las redes inalámbricas. | • Evalúe los diagramas de red.<br>• Evalúe las configuraciones de redes.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Se puede utilizar un(os) diagrama(s) de red vigente(s) u otra solución técnica o topológica que identifique las conexiones y dispositivos en la red para cumplir con este requisito. | | | | | | |
| **1.2.4** | Se mantienen diagramas de flujo de datos precisos que cumplen con lo siguiente:<br>• Muestran todos los flujos de datos del titular de la tarjeta a través de los sistemas y las redes involucradas.<br>• Se actualizan según sea necesario ante cambios en el ambiente. | • Evalúe el diagrama de flujo de datos.<br>• Observe las configuraciones de redes.<br>• Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Para cumplir con este requisito la entidad puede utilizar un diagrama de flujo de datos u otra solución técnica o topológica que identifique los flujos de datos del titular de la tarjeta a través de los sistemas y las redes. | | | | | | |
| **1.2.5** | Todos los servicios, protocolos y puertos permitidos están identificados, aprobados y tienen una necesidad de negocio definida. | • Evalúe la documentación.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.6** | Las configuraciones de seguridad son definidas e implementadas para todos los servicios, protocolos y puertos que están en uso y que son considerados inseguros, de tal manera que el riesgo es mitigado. | • Evalúe la documentación.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.2.7** | Las configuraciones de los NSC se revisan al menos una vez cada seis meses para confirmar que son pertinentes y eficientes. | • Evalúe los procedimientos documentados.<br>• Evalúe la documentación relativa a las revisiones desarrolladas.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **1.2.8** | Los archivos de configuración de los NSC están:<br>• Asegurados contra el acceso no autorizado.<br>• Se mantienen consistentes con las configuraciones de red activas. | • Evalúe los archivos de configuración del NSC. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Cualquier archivo o ajuste utilizado para configurar o sincronizar los NSC se considera un "archivo de configuración". Esto incluye archivos, controles automatizados y basados en el sistema, scripts, configuraciones, infraestructura como código u otros parámetros de los que se hace una copia de seguridad, se archivan o se almacenan de forma remota. | | | | | | |
| **1.3** El acceso a la red hacia y desde el entorno de datos de tarjetahabiente está restringido. | | | | | | | |
| **1.3.1** | El tráfico de entrada al CDE está restringido de la siguiente manera:<br>• Sólo al tráfico necesario.<br>• Todo el resto del tráfico está específicamente denegado. | • Evalúe los estándares de configuración del NSC.<br>• Evalúe las configuraciones del NSC. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.2** | El tráfico saliente del CDE se restringe de la siguiente manera:<br>• Sólo al tráfico necesario.<br>• Todo el resto del tráfico está específicamente denegado. | • Evalúe los estándares de configuración del NSC.<br>• Evalúe las configuraciones del NSC. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.3.3** | Los NSC se implementan entre todas las redes inalámbricas y el CDE; esto es independientemente de que la red inalámbrica sea parte CDE o no, de manera que:<br>• Todo el tráfico inalámbrico de las redes inalámbricas hacia el CDE es denegado de forma explícita.<br>• Sólo se permite el tráfico inalámbrico al CDE que tenga un propósito de negocio autorizado. | • Evalúe los ajustes de configuración.<br>• Evalúe los diagramas de red. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **1.4** Se controlan las conexiones de red entre las redes fiables y las que no lo son. | | | | | | | |
| **1.4.1** | Los NSC se implementan entre redes de confiables y no confiables. | • Evalúe los estándares de configuración del NSC.<br>• Evalúe los diagramas de redes vigentes.<br>• Evalúe las configuraciones de redes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **1.4.2** | El tráfico entrante de redes que no son confiables a redes confiables está restringido a:<br>• Las comunicaciones con componentes del sistema autorizados para proveer servicios de acceso público, protocolos y puertos.<br>• Respuestas las comunicaciones previamente iniciadas por componentes del sistema en una red confiable, esto para protocolos con dicho comportamiento.<br>• Todo el tráfico restante está denegado. | • Evalúe la documentación NSC.<br>• Evalúe las configuraciones del NSC. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>La intención de este requisito es abordar las sesiones de comunicación entre redes confiables y no confiables, en lugar de las especificaciones de los protocolos.<br><br>Este requisito no limita el uso de UDP u otros protocolos de red no orientados a conexión si el comportamiento estándar del estado de la conexión del protocolo es mantenido y bajo el control del NSC. | | | | | | |
| **1.4.3** | Se implementan medidas Antispoofing para detectar y bloquear la entrada a la red confiable de direcciones IP origen falsas o suplantadas. | • Evalúe la documentación NSC.<br>• Evalúe las configuraciones del NSC. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **1.4.4** | Los componentes del sistema que almacenan datos de tarjetahabiente no son accesibles directamente desde redes no confiables. | • Evalúe el diagrama de flujo de datos y el diagrama de red.<br>• Evalúe las configuraciones del NSC. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no se aplica al almacenamiento de datos del titular de la tarjeta en memoria volátil, pero sí se aplica cuando la memoria se trata como almacenamiento persistente (por ejemplo, disco RAM). Los datos del titular de la tarjeta sólo pueden almacenarse en la memoria volátil durante el tiempo necesario para soportar el proceso de negocio asociado (por ejemplo, hasta la finalización transacción relacionada con tarjeta de pago). | | | | | | |
| **1.4.5** | La divulgación de las direcciones IP internas y la información de enrutamiento se limita sólo a las partes autorizadas. | • Evalúe las configuraciones del NSC.<br>• Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|
| | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **1.5** Se mitigan los riesgos para el CDE desde dispositivos informáticos que pueden conectarse tanto a redes no confiables como al CDE. | | | | | | |
| **1.5.1** Los controles de seguridad se implementan en cualquier dispositivo informático, incluyendo los dispositivos propiedad de la empresa y de los empleados, que se conectan tanto a redes no confiables (incluida Internet) como al CDE manera siguiente:<br>• Se definen los parámetros de configuración específicos para impedir que se introduzcan amenazas en la red de la entidad.<br>• Los controles de seguridad se están ejecutando activamente.<br>• Los usuarios de los dispositivos informáticos no pueden alterar los controles de seguridad a menos que estén específicamente documentados y autorizados por el nivel gerencial, caso por caso, durante un período limitado. | • Evalúe las políticas y estándares de configuración.<br>• Evalúe los ajustes de configuración de los dispositivos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Notas de Aplicabilidad**<br><br>Estos controles de seguridad pueden desactivarse temporalmente solo si existe una necesidad técnica legítima, según lo autorizado por el nivel gerencial caso por caso. Se requiere de una autorización formal para desactivar estos controles de seguridad para y bajo un propósito específico. También puede ser necesario implementar medidas de seguridad adicionales durante el período en el cual estos controles seguridad estén desactivados.<br><br>Este requisito aplica a los dispositivos informáticos que sean propiedad tanto de la entidad como de los empleados. Los sistemas que no pueden ser administrados por políticas corporativas introducen debilidades y brindan oportunidades para que personas malintencionadas pueden explotarlas y/o aprovecharlas. | | | | | | |

## *Requisito 2: Aplicar Configuraciones Seguras a Todos los Componentes del Sistema*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **2.1** Se definen y comprenden los procesos y mecanismos para aplicar configuraciones seguras a todos los componentes del sistema. | | | | | | | |
| **2.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 2 están:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 2 son documentadas, asignadas y comprendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2** Los componentes del sistema se configuran y gestionan de forma segura. | | | | | | | |
| **2.2.1** | Los estándares de configuración se desarrollan, se implementan y se mantienen para:<br>• Cubrir todos los componentes del sistema.<br>• Cubrir todas las vulnerabilidades de seguridad conocidas.<br>• Brindar coherencia con el estándar de hardening del sistema aceptadas por el sector o con las recomendaciones de hardening del proveedor.<br>• Ser actualizadas a medida que se identifican nuevos problemas de vulnerabilidad, como se define en el requisito 6.3.1.<br>• Ser aplicadas cuando los nuevos sistemas sean configurados y verificadas como establecidas antes o inmediatamente después de que un componente del sistema se conecte a un entorno de producción. | • Evalúe los estándares de configuración del sistema.<br>• Revise los estándares de endurecimiento aceptados por la industria.<br>• Evalúe los ajustes de configuración.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **2.2.2** | Las cuentas predeterminadas del proveedor se gestionan de la siguiente manera:<br>• Si se utilizan las cuentas predeterminadas del proveedor, la contraseña predeterminada se cambia según el requisito 8.3.6.<br>• Si no se van a utilizar las cuentas predeterminadas del proveedor, la cuenta se elimina o se desactiva. | • Evalúe los estándares de configuración del sistema.<br>• Evalúe la documentación del proveedor.<br>• Observe a un administrador del sistema iniciando sesión con las cuentas predeterminadas del proveedor.<br>• Evalúe los archivos de configuración.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Esto se aplica a TODAS las cuentas y contraseñas predeterminadas del proveedor, incluidas, entre otras, las utilizadas por los sistemas operativos, el software que proporciona servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de punto de venta (POS), las aplicaciones de pago y los valores predeterminados del Protocolo Simple de Administración de Red (SNMP).<br><br>Este requisito también se aplica cuando un componente del sistema no está instalado en el entorno de una entidad, por ejemplo, el software y las aplicaciones que forman parte del CDE y a las que se ingresa a través de un servicio de suscripción en la nube. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **2.2.3** | Las funciones principales que requieren distintos niveles de seguridad se administran de la siguiente manera:<br>• Solo existe una función principal en un componente del sistema,<br>**O**<br>• Las funciones principales con distintos niveles de seguridad que existen en el mismo componente del sistema están aisladas entre sí,<br>**O**<br>• Las funciones principales con distintos niveles de seguridad en el mismo componente del sistema están todas aseguradas al nivel requerido por la función que requiera un nivel mayor de seguridad. | • Evalúe los estándares de configuración del sistema.<br>• Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.4** | Solo se habilitan los servicios, protocolos, demonios y funciones necesarios, y se eliminan o deshabilitan todas las funciones innecesarias. | • Evalúe los estándares de configuración del sistema.<br>• Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.5** | Si existen servicios, protocolos o «demonios» inseguros:<br>• La justificación comercial está documentada.<br>• Se documentan e implementan características de seguridad adicionales que reducen el riesgo de utilizar servicios, protocolos o "demonios" inseguros. | • Evalúe los estándares de configuración.<br>• Entreviste al personal.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2.2.6** | Los parámetros de seguridad del sistema están configurados para impedir su uso indebido. | • Evalúe los estándares de configuración del sistema.<br>• Entreviste al personal.<br>• Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **2.2.7** | Todo el acceso administrativo sin consola está cifrado utilizando criptografía robusta. | • Evalúe los estándares de configuración del sistema.<br>• Observe el inicio de sesión de un administrador.<br>• Evalúe las configuraciones del sistema.<br>• Evalúe la documentación del proveedor.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad** | | | | | | |
| | Esto incluye el acceso administrativo a través de interfaces basadas en navegador e interfaces de programación de aplicaciones (API). | | | | | | |
| **2.3** Los entornos inalámbricos se configuran y administran de forma segura. | | | | | | | |
| **2.3.1** | Para entornos inalámbricos conectados al CDE o que transmiten datos del titular de la tarjeta, todos los valores predeterminados de los proveedores inalámbricos se cambian en la instalación o se confirma que son seguros, incluidos, entre otros:<br>• Claves de cifrado inalámbricas predeterminadas.<br>• Contraseñas o puntos de acceso inalámbricos.<br>• Valores predeterminados de SNMP.<br>• Cualquier otro proveedor inalámbrico predeterminado relacionado con la seguridad. | • Evalúe las políticas y procedimientos.<br>• Revise la documentación del proveedor.<br>• Evalúe los ajustes de configuración inalámbrica.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad** | | | | | | |
| | Esto incluye, pero no se limita a, las claves de encriptación inalámbrica predeterminadas, las contraseñas de los puntos de acceso inalámbricos, los valores predeterminados de SNMP y cualquier otro valor predeterminado del proveedor inalámbrico relacionado con la seguridad. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **2.3.2** | Para los entornos inalámbricos conectados al CDE o que transmitan datos del titular de la tarjeta, las claves cifradas inalámbricas se cambian como sigue:<br>• Siempre que el personal con conocimiento de la clave deje la empresa o la función para la que era necesario el conocimiento.<br>• Siempre que se sospeche o se sepa que una clave está comprometida. | • Evalúe la documentación clave de administración.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |

# Proteger los Datos del Titular de la Tarjeta

## *Requisito 3: Proteger los Datos del Titular de la Tarjeta Almacenados*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.1** Se definen y comprenden los procesos y mecanismos para proteger los datos del titular de la tarjeta almacenados. | | | | | | | |
| **3.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 3 son:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 3 están documentadas, asignadas y comprendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.2** El almacenamiento de los datos del titular de la tarjeta se mantiene al mínimo. | | | | | | | |
| **3.2.1** | El almacenamiento de datos del titular de la tarjeta se mantiene al mínimo mediante la implementación de políticas y procedimientos de retención y eliminación de datos que incluyan al menos lo siguiente:<br>• Cobertura de todas las ubicaciones donde hay datos del titular de la tarjeta almacenados.<br>• Cobertura de cualquier dato de autenticación sensible (SAD) almacenado antes de completar la autorización. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; refiérase a las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.*<br>• Limitar la cantidad de datos almacenados y su tiempo de retención a lo requerido por los requisitos legales o reglamentarios y/o de negocios.<br>• Requisitos de retención específicos para los datos del titular de la tarjeta almacenados que definen la duración del período de retención e incluyen una justificación de negocio documentada.<br>• Procesos para el borrado seguro o para hacer que los datos del titular de la tarjeta que sean irrecuperables cuando ya no se necesitan según la política de retención.<br>• Un proceso para verificar, al menos una vez cada tres meses, que los datos del titular de la tarjeta almacenados que excedan el período de retención definido se han eliminado de forma segura o se han vuelto irrecuperables.<br><br>*(continuación)* | • Evalúe las políticas, procedimientos y procesos de conservación y eliminación de datos.<br>• Entreviste al personal.<br>• Evalúe los archivos y registros del sistema en los componentes del sistema en los que se almacenan los datos del titular de la tarjeta.<br>• Observe los mecanismos utilizados para hacer que los datos del titular de la tarjeta sean irrecuperables. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|
| | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **Notas de Aplicabilidad** | | | | | | |
| Cuando un TPSP almacena datos del titular de la tarjeta (por ejemplo, en un entorno de nube), las entidades son responsables de trabajar con sus proveedores de servicios para comprender cómo el TPSP cumple con este requisito para la entidad. Las consideraciones incluyen garantizar que todas las instancias geográficas de un elemento de datos se eliminen de forma segura.<br>*El punto anterior (para la cobertura de SAD almacenada antes de completar la autorización) es una mejor práctica hasta el 31 de marzo de 2025, después de lo cual se requerirá como parte del Requisito 3.2.1 y se debe considerar en su totalidad durante una evaluación de los PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.3** Los datos de autenticación sensibles (SAD) no se almacenan después de la autorización. | | | | | | | |
| **3.3.1** | Los SAD no se almacenan después de la autorización, incluso si están cifrados. Todos los datos de autenticación sensibles recibidos se vuelven irrecuperables una vez finalizado el proceso de autorización. | • Evalúe las políticas y procedimientos documentados.<br>• Evalúe las configuraciones del sistema.<br>• Observe los procesos de eliminación de datos seguros. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br>*Parte de esta Nota de Aplicabilidad se eliminó intencionadamente para este SAQ, ya que no se aplica a las evaluaciones de las empresas.*<br>Los datos de autenticación sensibles incluyen los datos citados en los Requisitos 3.3.1.1 hasta el 3.3.1.3. | | | | | | |
| **3.3.1.1** | El contenido completo de cualquier pista no se almacena una vez finalizado el proceso de autorización. | • Evalúe las fuentes de datos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br>En el curso normal de los negocios, es posible que sea necesario conservar los siguientes elementos de datos de la pista:<br>• Nombre del tarjetahabiente.<br>• Número de cuenta principal (PAN).<br>• Fecha de expiración.<br>• Código de servicio.<br>Para minimizar el riesgo, almacene de forma segura sólo estos elementos de datos según sea necesario para la empresa. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.3.1.2** | El código de verificación de la tarjeta no se almacena una vez finalizado el proceso de autorización. | • Evalúe las fuentes de datos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El código de verificación de la tarjeta es el número de tres o cuatro dígitos impresos en el anverso o reverso de una tarjeta de pago, que se utiliza para verificar las transacciones sin tarjeta presente. | | | | | | |
| **3.3.1.3** | El número de identificación personal (PIN) y el bloque del PIN no se almacenan una vez finalizado el proceso de autorización. | • Evalúe las fuentes de datos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Los bloques PIN se cifran durante el curso natural de los procesos de transacción, pero incluso si una entidad cifra el bloque de PIN nuevamente, todavía no se permite que se almacene después de la finalización del proceso de autorización. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.3.2** | Los SAD que se almacenan electrónicamente antes de completar la autorización se cifran mediante criptografía robusta. | • Evalúe los almacenajes de datos y las configuraciones del sistema.<br>• Evalúe la documentación del proveedor. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Las organizaciones que administran los programas de cumplimiento (por ejemplo, las marcas de pago y adquirentes) determinan si se permite el almacenamiento de los SAD antes de la autorización. Comuníquese con estas organizaciones para cualquier criterio adicional.<br><br>Este requisito aplica para todo almacenamiento de los SAD, incluso si no hay datos PAN en el entorno.<br><br>Consulte el Requisito 3.2.1 para conocer el requisito adicional que aplica si el SAD se almacena antes de completar la autorización.<br><br>*Parte de esta Nota de Aplicabilidad se eliminó intencionadamente para este SAQ, ya que no se aplica a las evaluaciones de las empresas.*<br><br>Este requisito no reemplaza la forma en que se deben administrar los bloques de PIN, ni significa que un bloque de PIN que haya sido cifrado correctamente deba volver a cifrarse.<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **3.3.3** | ***Requisito adicional para emisores y empresas que soportan servicios de emisión y que almacenan datos de autenticación sensibles.*** | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.4** El acceso a las pantallas de datos PAN completas y la capacidad de copiar los datos PAN están restringidos. | | | | | | | |
| **3.4.1** | Los datos PAN están enmascarados cuando se muestra (el BIN y los últimos cuatro dígitos constituyen **el número máximo** de dígitos que se muestran), de manera que sólo el personal con una necesidad legítima de negocios pueda ver **más que** el BIN y los últimos cuatro dígitos de los datos PAN. | • Evalúe las políticas y procedimientos documentados.<br>• Evalúe las configuraciones del sistema.<br>• Evalúe la lista documentada de los roles que necesitan tener acceso a algo más que el BIN y a los últimos cuatro dígitos del PAN (incluye el PAN completo).<br>• Evalúe la presentación del PAN (por ejemplo, en la pantalla, en los recibos de papel). | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no sustituye a otros más estrictos para la visualización de los datos de tarjetahabiente, por ejemplo, los requisitos legales o de las marcas de pago para los recibos de los puntos de venta (POS).<br>Este requisito se refiere a la protección de los datos PAN cuando se muestran en pantallas, recibos de papel, impresiones, etc., y no debe confundirse con el requisito 3.5.1 para la protección de los datos PAN cuando se almacenan, procesan o transmiten. | | | | | | |
| **3.4.2** | Cuando se utilicen tecnologías de acceso remoto, los controles técnicos impiden la copia y/o la reubicación de los datos PAN para todo el personal, excepto para aquellos con autorización explícita y documentada y una necesidad legítima de negocio y definida. | • Evalúe las políticas, procedimientos y evidencias documentados de los controles técnicos.<br>• Evalúe las configuraciones de las tecnologías de acceso remoto.<br>• Observe los procesos.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Almacenar o reubicar los datos PAN en discos duros locales, medios electrónicos extraíbles y otros dispositivos de almacenamiento hace que estos dispositivos estén dentro del alcance PCI DSS.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.5** El número de cuenta principal (PAN) está protegido donde sea que se almacene. | | | | | | | |
| **3.5.1** | Los datos PAN se hacen ilegibles en cualquier lugar donde se almacenen utilizando cualquiera de los siguientes enfoques:<br>• *Hashes* unidireccionales basados en criptografía robusta del PAN completo.<br>• Truncamiento (los hashes no pueden utilizarse para reemplazar el segmento truncado de la PAN).<br>– Si en un entorno hay versiones truncadas y con hash del mismo PAN, o diferentes formatos de truncamiento del mismo PAN, se establecen controles adicionales de manera que las diferentes versiones no puedan correlacionarse para reconstruir el PAN original.<br>• Indice de tokens.<br>• Criptografía robusta con procesos y procedimientos de gestión de claves asociados. | • Evalúe la documentación sobre el sistema utilizado para hacer ilegible el PAN.<br>• Evalúe los depósitos de datos.<br>• Evalúe los registros de auditoría, incluyendo los registros de aplicaciones de pago.<br>• Evalúe los controles para verificar que los PAN cifrados y truncados no pueden correlacionarse para reconstruir el PAN original. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito se aplica a los datos PAN guardados en almacenamiento primario (bases de datos o archivos planos como hojas de cálculo de archivos de texto), así como en almacenamiento no primario (copias de seguridad, registros de auditoría, registros de excepciones o de resolución de problemas).<br>Este requisito no excluye el uso de archivos temporales que contengan datos PAN en texto no cifrado mientras se encriptan y des-encriptan. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.5.1.1** | Los *hash* utilizados para hacer ilegibles los datos PAN (según el primer punto del requisito 3.5.1) son hashes criptográficos con clave de todos los datos PAN, con procesos y procedimientos de gestión de claves asociados de acuerdo con los Requisitos 3.6 y 3.7. | • Evalúe la documentación sobre el método de *hash* utilizado.<br>• Evalúe la documentación sobre los procedimientos y procesos de gestión de claves.<br>• Evalúe los depósitos de datos.<br>• Evalúe los registros de auditoría, incluyendo los registros de aplicaciones de pago. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Todas las Notas de Aplicabilidad del Requisito 3.5.1. se aplican también este requisito.<br><br>Los procesos y procedimientos de gestión de claves (Requisitos 3.6 y 3.7) no se aplican a los componentes del sistema utilizados para generar hashes con clave individuales de un PAN para su comparación con otro sistema si:<br>• Los componentes del sistema solo tienen acceso a un valor de hash a la vez (los valores de hash no se almacenan en el sistema)<br>**Y**<br>• No hay otros datos de cuenta almacenados en el mismo sistema que los hashes.<br>*Este requisito se considera una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS. Este requisito reemplazará el punto del Requisito 3.5.1 para hashes unidireccionales una vez que se alcance su fecha de efectividad.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.5.1.2** | Si se utiliza un a nivel de disco o de partición (en lugar de un cifrado de base de datos a nivel de archivo, columna o campo) para hacer que los datos PAN sea ilegibles, sólo se implementará de la siguiente manera:<br>• En medios electrónicos extraíbles,<br>**O**<br>• Si se utiliza para medios electrónicos no extraíbles, los datos PAN también se hacen ilegibles mediante otro mecanismo que cumpla con el Requisito 3.5.1. | • Observe los procesos de cifrado.<br>• Evalúe las configuraciones y/o la documentación del proveedor.<br>• Observe los procesos de cifrado. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito se aplica a cualquier método de cifrado que proporcione automáticamente un PAN en texto claro cuando se ejecuta un sistema, aunque un usuario autorizado no haya solicitado específicamente esos datos.<br>Aunque el cifrado de disco puede seguir estando presente en estos tipos de dispositivos, este no puede ser el único mecanismo utilizado para proteger los datos del PAN almacenados en esos sistemas. Cualquier dato del PAN almacenado también debe volverse ilegible según el Requisito 3.5.1, por ejemplo, mediante el truncamiento o por un mecanismo de cifrado a nivel de datos. El cifrado de disco completo ayuda a proteger los datos en caso de pérdida física de un disco y, por lo tanto, su uso es apropiado sólo para dispositivos de almacenamiento de medios electrónicos extraíbles.<br>Los medios que forman parte de la arquitectura de un centro de datos (por ejemplo, unidades intercambiables en caliente, copias de seguridad en cinta) se consideran medios electrónicos no extraíbles a los que se aplica el Requisito 3.5.1.<br>Las implementaciones de cifrado de discos o particiones también deben cumplir todos los demás requisitos de cifrado y gestión de claves PCI DSS.<br>*Parte de esta Nota de Aplicabilidad se eliminó intencionadamente para este SAQ, ya que no se aplica a las evaluaciones de las empresas.*<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.5.1.3** | Si se utiliza el cifrado a nivel del disco o de partición (en lugar del cifrado de la base de datos a nivel de archivo, columna o campo) para hacer que los datos PAN sea ilegibles, sólo se implementará de la siguiente manera:<br>• El acceso lógico se gestiona por separado e independientemente de la autenticación del sistema operativo nativo y de los mecanismos de control de acceso.<br>• Las claves de descifrado no están asociadas a las cuentas de usuario.<br>• Los factores de autenticación (contraseñas, frases de paso o claves criptográficas) que permiten el acceso a los datos no cifrados se almacenan de forma segura. | • Evalúe las configuraciones del sistema.<br>• Observe el proceso de autenticación.<br>• Evalúe los archivos que contienen factores de autenticación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Las implementaciones de cifrado de discos o particiones también deben cumplir todos los demás requisitos de cifrado y gestión de claves PCI DSS. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.6** Las claves criptográficas utilizadas para proteger los datos del titular de la tarjeta almacenados están protegidos. | | | | | | | |
| **3.6.1** | Los procedimientos se definen e implementan para proteger las claves cifradas utilizadas para proteger los datos del titular de la tarjeta almacenados contra la divulgación y el uso indebido que incluyen:<br>• El acceso a las claves está restringido al menor número de custodios necesarios.<br>• Las claves de cifrado de claves son al menos tan seguras como las claves de cifrado de datos que estas protegen.<br>• Las claves de cifrado de claves se almacenan por separado de las claves de cifrado de datos.<br>• Las claves se almacenan de forma segura en el menor número posible de formas y ubicaciones. | • Evalúe las políticas y procedimientos documentados de gestión de claves. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito se aplica a las claves utilizadas para proteger los datos del titular de la tarjeta almacenados y a las claves de cifrado utilizadas para proteger las claves de cifrado de datos.<br>El requisito para proteger las claves utilizadas para proteger los datos del titular de la tarjeta almacenados de la divulgación y el uso indebido se aplica tanto a las claves de cifrado de datos como a las claves de cifrado de claves. Debido a que una clave de cifrado de claves puede otorgar acceso a muchas claves de cifrado de datos, las claves de cifrado de claves requieren fuertes medidas de protección. | | | | | | |
| **3.6.1.1** | *Requisito adicional sólo para proveedores de servicios.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.6.1.2** | Las claves secretas y privadas que se utilizan para proteger los datos del titular de la tarjeta se almacenan en uno (o más) de las siguientes formas en todo momento:<br>• Cifrado con una clave de cifrado de clave, que sea al menos tan fuerte, como la clave de cifrado de datos y que se almacene por separado de la clave de cifrado de datos.<br>• Dentro de un dispositivo criptográfico seguro (SCD), como un módulo de seguridad de hardware (HSM) o un dispositivo de punto de interacción aprobado por PTS.<br>• Como, al menos, dos componentes de clave de longitud completa o claves compartidas de acuerdo con un método aceptado por la industria. | • Evalúe los procedimientos documentados.<br>• Evalúe las configuraciones del sistema y las ubicaciones de almacenamiento de claves, incluyendo para las claves de cifrado de claves. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>No es necesario que las claves públicas sean almacenadas en una de estas formas.<br>Las claves criptográficas almacenadas como parte de un sistema de gestión de claves (KMS) que emplea SCD son aceptables.<br>Una clave criptográfica que se divide en dos partes no cumple con este requisito. Las claves secretas o privadas almacenadas como componentes clave o recursos compartidos de claves deben generarse a través de uno de los siguientes:<br>• Utilizando un generador de números aleatorios aprobado y dentro de un SCD,<br>**O**<br>• De acuerdo con el estándar ISO 19592 o su equivalente en la industria para la generación de claves secretas compartidas. | | | | | | |
| **3.6.1.3** | El acceso a los componentes de claves criptográficas de texto no cifrado está restringido al menor número posible de custodios que sean necesarios. | • Evalúe las listas de acceso de los usuarios. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.6.1.4** | Las claves criptográficas se almacenan en el menor número posible de ubicaciones. | • Evalúe las locaciones clave almacenamiento.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.7** Cuando se usa criptografía para proteger datos del titular de la tarjeta almacenados, se definen e implementan procesos y procedimientos de administración de claves que cubren todos los aspectos del ciclo de vida de las claves. | | | | | | | |
| **3.7.1** | Las políticas y procedimientos de administración de claves se implementan para incluir la generación de claves criptográficas fuertes utilizadas para proteger los datos del titular de la tarjeta almacenados. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Observe el método de generación de claves. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.7.2** | Las políticas y los procedimientos de administración de claves son implementados para incluir la distribución segura de las claves criptográficas utilizadas para proteger los datos del titular de la tarjeta almacenados. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Observe el método de distribución de claves. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.7.3** | Se implementan políticas y procedimientos de gestión de claves para incluir el almacenamiento seguro de las claves criptográficas utilizadas para proteger los datos del titular de la tarjeta almacenados. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Observe el método de almacenamiento de claves. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.7.4** | Se implementan políticas y procedimientos de gestión de claves para los cambios de claves criptográficas de aquellas claves que han llegado al final de su criptoperíodo, según lo definido por el proveedor de la aplicación asociada o por el propietario de la clave, y basado en las mejores prácticas y lineamientos de la industria, incluyendo lo siguiente:<br>• Un criptoperíodo definido para cada tipo de clave en uso.<br>• Un proceso para el cambio de claves al final del criptoperíodo definido. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Entreviste al personal.<br>• Observe las locaciones clave de almacenamiento. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.7.5** | Los procedimientos de políticas de gestión de claves se implementan para incluir el retiro, sustitución o destrucción de las claves utilizadas para proteger los datos del titular de la tarjeta almacenados, según se considere necesario cuando:<br>• La clave haya llegado al final de su criptoperíodo definido.<br>• La integridad de la clave se haya debilitado, incluso cuando el personal con conocimiento de un componente de la clave en texto no cifrado abandone la empresa, o la función por la que conocía la clave.<br>• Se sospecha o se sabe que la clave está comprometida.<br>Las claves retiradas o reemplazadas no se utilizan para operaciones de cifrado. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Si es necesario conservar las claves criptográficas retiradas o reemplazas, dichas claves deben archivarse de forma segura (por ejemplo, utilizando una clave de cifrado). | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **3.7.6** | Cuando el personal realiza operaciones manuales de gestión de claves criptográficas en texto no cifrado, se implementan políticas y procedimientos de gestión de claves que incluyen la gestión de estas operaciones utilizando conocimiento dividido y control dual. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Entreviste al personal.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este control es aplicable para operaciones manuales de administración de claves.<br>Una clave criptográfica que simplemente se divide en dos partes no cumple con este requisito. Las claves secretas o privadas almacenadas como componentes clave o recursos compartidos de claves deben generarse a través de uno de los siguientes métodos:<br>• Utilizando un generador de números aleatorios aprobado y dentro de un dispositivo criptográfico seguro (SCD), como un módulo de seguridad de hardware (HSM) o un dispositivo de punto de interacción aprobado por PTS,<br>**O**<br>• De acuerdo con el Estándar ISO 19592 o su equivalente en la industria para la generación de claves secretas compartidas. | | | | | | |
| **3.7.7** | Se implementan políticas y procedimientos de administración de claves para incluir la prevención de la sustitución no autorizada de claves criptográficas. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Entreviste al personal.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.7.8** | Las políticas y los procedimientos de administración de claves se implementan para incluir que los custodios de claves criptográficas reconozcan formalmente (por escrito o electrónicamente) que comprenden y aceptan sus responsabilidades como custodios de claves. | • Evalúe las políticas y procedimientos documentados de gestión de claves.<br>• Revise la documentación u otras evidencias de los reconocimientos de los custodios clave. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3.7.9** | *Requisito adicional sólo para proveedores de servicios* | | | | | | |

## *Requisito 4: Proteger los Datos de Tarjetahabiente con Criptografía Robusta Durante la Transmisión a Través de Redes Abiertas y Públicas*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **4.1** Los procesos y mecanismos para proteger los datos de tarjetahabiente con criptografía robusta durante la transmisión a través de redes públicas abiertas están definidos y comprendidos. | | | | | | | |
| **4.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 4 son:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 4 están documentadas, asignadas y comprendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **4.2** Los datos PAN está protegidos con criptografía robusta durante la transmisión. | | | | | | | |
| **4.2.1** | Se implementan fuertes protocolos de seguridad y criptografía de la siguiente manera para proteger los datos PAN durante la transmisión a través de redes públicas abiertas: | | | | | | |
| | • Sólo se aceptan claves y certificados confiables. | • Evalúe las políticas y procedimientos documentados.<br>• Entreviste al personal.<br>• Evalúe las configuraciones del sistema.<br>• Evalúe las transmisiones de datos de tarjetahabiente.<br>• Evalúe las claves y los certificados. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Los certificados utilizados para proteger los datos PAN durante la transmisión a través de redes públicas abiertas se confirman como válidos y no están vencidos ni revocados. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; consulte las notas de aplicabilidad a continuación para obtener más detalles.* | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • El protocolo en uso sólo admite versiones o configuraciones seguras y no admite el apoyo ni el uso de versiones, algoritmos, tamaños de clave o implementaciones inseguras. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • La fuerza del cifrado es apropiada para la metodología de cifrado en uso. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Un certificado auto-firmado también puede ser aceptable si el certificado es emitido por una CA interna dentro de la organización, si el autor del certificado está confirmado y si el certificado está verificado (por ejemplo, mediante hash o firma) y no está caducado.<br><br>*El punto anterior (para confirmar que los certificados utilizados para proteger los datos PAN durante la transmisión a través de redes públicas abiertas son válidos y no están vencidos ni revocados) es una mejor práctica hasta el 31 de marzo de 2025, después de lo cual se requerirá como parte del Requisito 4.2.1 y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **4.2.1.1** | Se mantiene un inventario de las caves y certificados confiables de la entidad utilizados para proteger los datos PAN durante la transmisión. | • Evalúe las políticas y procedimientos documentados.<br>• Evalúe el inventario de claves y certificados confiables. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **4.2.1.2** | Las redes inalámbricas que transmiten datos PAN o están conectadas al CDE utilizan las mejores prácticas de la industria para implementar criptografía robusta para autenticación y transmisión. | • Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4.2.2** | Los datos PAN están protegidos con criptografía robusta siempre que se envíen a través de tecnologías de mensajería para el usuario final. | • Evalúe las políticas y procedimientos documentados.<br>• Evalúe las configuraciones del sistema y la documentación del proveedor. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito también se aplica si un cliente, u otro tercero, solicita que se le envíe datos PAN a través de tecnologías de mensajería de usuario final.<br>Pueden darse casos en los que una entidad reciba datos de tarjetahabiente no solicitados a través de un canal de comunicación inseguro que no estaba destinado a la transmisión de datos sensibles. Ante esta situación, la entidad puede optar por incluir el canal en el ámbito de su CDE y protegerlo de acuerdo con PCI DSS o eliminar los datos de tarjetahabiente e implementar medidas para evitar que el canal se utilice para los datos de tarjetahabiente. | | | | | | |

# Mantener un Programa de Gestión de Vulnerabilidades

## *Requisito 5: Proteger Todos los Sistemas y Redes de Software Malicioso*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **5.1** Se definen y comprenden los procesos y mecanismos para proteger todos los sistemas y redes del software malintencionado. | | | | | | | |
| **5.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 5 son:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 5 están documentadas, asignadas y comprendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.2** El software malintencionado *(malware)* es evadido, o se detecta y se soluciona. | | | | | | | |
| **5.2.1** | Una solución *antimalware* se aplicará a todos los componentes del sistema, excepto a aquellos componentes del sistema identificados en evaluaciones periódicas según el Requisito 5.2.3 que concluye que los componentes del sistema no están en riesgo de *malware.* | • Evalúe los Componentes del Sistema.<br>• Evalúe las evaluaciones periódicas. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.2.2** | Las soluciones *antimalware* implementadas:<br>• Detectan todos los tipos conocidos de *malware.*<br>• Eliminan, bloquean o contienen todos los tipos conocidos de *malware.* | • Evalúe la documentación del proveedor.<br>• Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **5.2.3** | Todos los componentes del sistema que no se encuentren en riesgo de *malware* se evalúan periódicamente para incluir lo siguiente:<br>• Una lista documentada de todos los componentes del sistema que no están en riesgo de *malware.*<br>• Identificación y evaluación de amenazas de *malware* en evolución para los componentes del sistema.<br>• Confirmación de si dichos componentes del sistema continúan sin requerir protección *antimalware*. | • Evalúe las políticas y procedimientos documentados.<br>• Entreviste al personal.<br>• Evalúe la lista de los componentes del sistema que no corren riesgo de sufrir *malware* y compárela contra los componentes del sistema que no cuenten con una solución antimalware. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Los componentes del sistema cubiertos por este requisito son aquellos para los que no existe una solución *antimalware* implementada según el Requisito 5.2.1. | | | | | | |
| **5.2.3.1** | La frecuencia de las evaluaciones periódicas de los componentes del sistema identificados como no en riesgo de *malware* se define en el análisis de riesgo específico de la entidad, el cual se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1. | • Evalúe el análisis de riesgos específico.<br>• Evalúe los resultados documentados de las evaluaciones periódicas.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **5.3** Los mecanismos y procesos *antimalware* están activos, son mantenidos y monitoreados. | | | | | | | |
| **5.3.1** | Las soluciones *antimalware* se mantienen actualizadas a través de procesos de actualización automáticos. | • Evalúe las soluciones antimalware incluyendo cualquier instalación maestra.<br>• Evalúe los Componentes y Registros del Sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **5.3.2** | Soluciones *antimalware*:<br>• Realizan escaneos periódicos y escaneos activos o en tiempo real<br>O<br>• Realizan un análisis continuo del comportamiento de los sistemas o procesos. | • Evalúe las soluciones antimalware incluyendo cualquier instalación maestra.<br>• Evalúe los Componentes del Sistema.<br>• Evalúe los resultados de registros y escaneos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.3.2.1** | Si se realizan escaneos periódicos de *malware* para cumplir con el requisito 5.3.2, la frecuencia de los escaneos se define en el análisis de riesgos específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1. | • Evalúe el análisis de riesgos específico.<br>• Evalúe los resultados documentados de los escaneos de malware.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br>Este requisito aplica para las entidades que realizan escaneos periódicos de *malware* para cumplir con el Requisito 5.3.2.<br>Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS. | | | | | | |
| **5.3.3** | Para los medios electrónicos extraíbles, la solución *antimalware*:<br>• Realiza escaneos automáticos cuando el medio es insertado, conectado o montado lógicamente,<br>**O**<br>• Realiza un análisis continuo del comportamiento de los sistemas o procesos cuando el medio está insertado, conectado o montado lógicamente. | • Evalúe las configuraciones de las soluciones *antimalware.*<br>• Evalúe los componentes del sistema con medios electrónicos removibles.<br>• Evalúe los resultados de registros y escaneos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **5.3.4** | Los registros de auditoría de la solución *antimalware* están habilitados y se conservan de acuerdo con el requisito 10.5.1. | • Evalúe las configuraciones de las soluciones *antimalware.* | ☐ | ☐ | ☐ | ☐ | ☐ |
| **5.3.5** | Los mecanismos *antimalware* no pueden ser desactivados o alterados por los usuarios, a menos que esté específicamente documentado y autorizado por la administración en cada caso, por un período de tiempo limitado. | • Evalúe las configuraciones *antimalware.*<br>• Observe los procesos.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Las soluciones *antimalware* sólo pueden desactivarse temporalmente si existe una necesidad técnica legítima, autorizada por la dirección en cada caso. Si es necesario desactivar la protección *antimalware* para un fin específico, esto debe ser formalmente autorizado. También puede ser necesario implementar medidas de seguridad adicionales para el período durante el cual la protección *antimalware* no está activa. | | | | | | |
| **5.4** Los mecanismos contra *phishing* protegen a los usuarios contra los ataques de *phishing*. | | | | | | | |
| **5.4.1** | Existen procesos y mecanismos automatizados para detectar y proteger al personal contra ataques de *phishing.* | • Observe los procesos implementados.<br>• Evalúe los mecanismos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El enfoque de este requisito es proteger al personal con acceso a los componentes del sistema en el ámbito PCI DSS.<br>Cumplir con este requisito de controles técnicos y automatizados para detectar y proteger al personal contra el phishing no es igual a lo que establece el Requisito 12.6.3.1 en cuanto al entrenamiento de concienciación sobre seguridad. Cumplir con este requisito tampoco implica que se está cumpliendo con el requisito de proporcionar al personal capacitación en cuanto a concienciación de seguridad, y viceversa.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

## *Requisito 6: Desarrollar y Mantener Sistemas y Softwares Seguros*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.1** Se definen y comprenden los procesos y mecanismos para desarrollar y mantener sistemas y software seguros. | | | | | | | |
| **6.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 6 son:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 6 están documentadas, asignadas y comprendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.2** El software a medida y personalizado se desarrolla de forma segura. | | | | | | | |
| **6.2.1** | El software a medida y personalizado se desarrolla de forma segura, de la siguiente manera:<br>• Basándose en los estándares de la industria y/o mejores prácticas para un desarrollo seguro.<br>• De acuerdo con los PCI DSS (por ejemplo, autenticación segura y registro).<br>• Incorporar la consideración de la información de problemas de seguridad durante cada etapa del ciclo de vida del desarrollo de software. | • Evalúe los procedimientos documentados de desarrollo de software. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Esto aplica a todo el software desarrollado por o para la entidad para su propio uso. Esto incluye software tanto a la medida como personalizado. Esto no aplica para el software de terceros. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.2.2** | El personal de desarrollo de software que trabaja en software a medida y personalizado recibe capacitación al menos una vez cada 12 meses de la siguiente manera:<br>• Sobre la seguridad de software relevante para su función laboral y lenguajes de desarrollo.<br>• Incluyendo diseño de software seguro y técnicas de codificación segura.<br>• Incluyendo, si se utilizan herramientas de prueba de seguridad, cómo utilizar las herramientas para detectar vulnerabilidades en el software. | • Evalúe los procedimientos documentados de desarrollo de software.<br>• Evalúe los registros de entrenamiento.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El personal de desarrollo de software sigue estando informado sobre las prácticas de desarrollo seguras; seguridad de software; y ataques contra los lenguajes, marcos o aplicaciones que desarrollan. El personal puede recibir asistencia y orientación cuando sea necesario. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.2.3** | El software a la medida y personalizado es revisado antes de ser lanzado a producción o para los clientes, a fin de identificar y corregir posibles vulnerabilidades de codificación, de la siguiente manera:<br>• Las revisiones de código garantizan que el código se desarrolle de acuerdo con las pautas de codificación segura.<br>• Las revisiones de código buscan vulnerabilidades de software tanto existentes como emergentes.<br>• Las correcciones apropiadas se implementan antes de la publicación. | • Evalúe los procedimientos documentados de desarrollo de software.<br>• Entreviste al personal responsable.<br>• Evalúe las evidencias de los cambios en el software a medida y personalizado. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito para las revisiones de código se aplica a todo el software a medida y personalizado (tanto interno como público), como parte del ciclo de vida de desarrollo del sistema.<br>Las aplicaciones web públicas también están sujetas a controles adicionales para abordar las amenazas y vulnerabilidades continuas después de la implementación, como se define en el Requisito 6.4 PCI DSS.<br>Las revisiones de código se pueden realizar mediante procesos manuales o automatizados, o una combinación de ambos. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.2.3.1** | Si las revisiones manuales de código son realizadas para software hecho a medida y personalizado antes de ser liberado a producción, los cambios de código son:<br>• Revisados por personas que no sean el autor del código original, y que conozcan las técnicas de revisión de código y las prácticas de codificación segura.<br>• Revisados y aprobados por la dirección antes de su publicación. | • Evalúe los procedimientos documentados de desarrollo de software.<br>• Entreviste al personal responsable.<br>• Evalúe las evidencias de los cambios en el software a medida y personalizado. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Las revisiones manuales de código pueden ser llevadas a cabo por personal interno con conocimientos o por personal de terceros con conocimientos.<br>Una persona a la que se le ha concedido formalmente la responsabilidad del control de la publicación y que no es ni el autor original del código ni el revisor del mismo cumple con los criterios de ser administrador. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.2.4** | Las técnicas de ingeniería de software u otros métodos están definidos y en uso para el software a medida y personalizado por el personal de desarrollo de software a fin de impedir o mitigar los ataques de software comunes y las vulnerabilidades relacionadas, incluyendo, pero no limitado a lo siguiente: | | | | | | |
| | • Ataques de inyección, incluyendo SQL, LDAP, XPath u otros fallos de tipo comando, parámetro, objeto, defecto o de inyección. | • Evalúe los procedimientos documentados.<br>• Entreviste al personal responsable por el desarrollo de software. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Ataques a datos y estructuras de datos, incluyendo intentos de manipulación de buffers, punteros, datos de entrada o datos compartidos. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Ataques al uso de criptografía, incluyendo intentos de explotar implementaciones criptográficas débiles, inseguras o inapropiadas, algoritmos, suites de cifrado o modos de operación. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Ataques a la lógica del negocio, incluyendo los intentos de abusar o eludir las características y funcionalidades de la aplicación a través de la manipulación de las APIs, los protocolos y canales de comunicación, la funcionalidad del lado del cliente, u otras funciones y recursos del sistema/aplicación. Esto incluye los scripts entre sitios (XSS) y la falsificación de petición entre sitios (CSRF).<br><br>*(continuación)* | | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.2.4** | • Ataques a los mecanismos de control de acceso, incluidos los intentos de eludir o abusar de los mecanismos de identificación, autenticación o autorización, o los intentos de aprovechar las debilidades en la implementación de dichos mecanismos. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Ataques a través de cualquier vulnerabilidad de "alto riesgo" identificada en el proceso de identificación de vulnerabilidades, tal como se define en el Requisito 6.3.1. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Esto se aplica a todo el software desarrollado por o para la entidad para su propio uso. Esto incluye software tanto a medida como personalizado. Esto no aplica para el software de terceros. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.3** Las vulnerabilidades de seguridad se identifican y son abordadas. | | | | | | | |
| **6.3.1** | Las vulnerabilidades de seguridad se identifican y gestionan de la siguiente manera:<br>• Las nuevas vulnerabilidades de seguridad se identifican utilizando fuentes reconocidas por la industria de información de vulnerabilidades de seguridad, incluyendo alertas de equipos internacionales y nacionales de respuesta a emergencias informáticas (CERTs).<br>• A las vulnerabilidades se les asigna una clasificación de riesgo basada en las mejores prácticas de la industria y considerando su impacto potencial.<br>• Las clasificaciones de riesgo identifican, como mínimo, todas las vulnerabilidades consideradas de alto riesgo o críticas para el entorno.<br>• Se cubren las vulnerabilidades de los programas informáticos a medida y de terceros (por ejemplo, sistemas operativos y bases de datos). | • Evalúe las políticas y procedimientos.<br>• Entreviste al personal responsable.<br>• Evalúe la documentación.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no se consigue con los escaneos, y es adicional a la realización de los escaneos de vulnerabilidades realizados para los Requisitos 11.3.1 y 11.3.2. Este requisito se refiere a un proceso para monitorizar activamente las fuentes de la industria en materia de información de vulnerabilidades y para que la entidad determine la clasificación de riesgo que se asociará con cada vulnerabilidad. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.3.2** | A fin de facilitar la gestión de vulnerabilidades y parches se mantiene un inventario del software a medida y personalizado y de los componentes del software de terceros incorporados en el software a medida y personalizado. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **6.3.3** | Todos los componentes del sistema están protegidos contra vulnerabilidades conocidas mediante la instalación de parches /actualizaciones de seguridad aplicables de la siguiente manera:<br>• Los parches/actualizaciones para vulnerabilidades críticas (identificados de acuerdo con el proceso de clasificación de riesgos del Requisito 6.3.1) se instalan dentro del período de un mes de su emisión.<br>• Todos los demás parches/actualizaciones de seguridad aplicables se instalan dentro de un período de tiempo apropiado según determine la entidad de acuerdo a la evaluación de la criticidad del riesgo para el entorno, tal como se identifica en el proceso de clasificación de riesgos del Requisito 6.3.1. | • Evalúe las políticas y procedimientos.<br>• Evalúe los componentes del sistema y software relacionado.<br>• Compare la lista de parches de seguridad instalados con las listas de parches del proveedor recientes. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.4** Las aplicaciones web públicas están protegidas contra ataques. | | | | | | | |
| **6.4.1** | Para las aplicaciones web de cara al público, las nuevas amenazas y vulnerabilidades se abordan de forma continua y están protegidas contra los ataques conocidos de la siguiente manera:<br>• Revisión de las aplicaciones web de cara al público mediante herramientas o métodos de evaluación de la seguridad de las vulnerabilidades de las aplicaciones, sean manuales o automatizadas, como sigue:<br>– Al menos una vez cada 12 meses y después de cambios significativos.<br>– Por una entidad especializada en seguridad de aplicaciones.<br>– Incluyendo, como mínimo, todos los ataques de software comunes descritos en el Requisito 6.2.4.<br>– Todas las vulnerabilidades se clasifican de acuerdo con el Requisito 6.3.1.<br>– Se corrigen todas las vulnerabilidades.<br>– La aplicación se vuelve a examinar después de las correcciones.<br>*(continuación)* | • Evalúe los procesos documentados.<br>• Entreviste al personal.<br>• Evalúe los registros de las evaluaciones de seguridad de las aplicaciones.<br>• Evalúe los ajustes de configuración del sistema y los registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.4.1** | **O**<br>• Instalación de soluciones técnicas automatizadas que detecten e impidan continuamente los ataques basados en la web de la siguiente manera:<br>– Instaladas frente a las aplicaciones web de públicas para detectar e impedir los ataques basados en la web.<br>– Funcionando activamente y actualizándose según corresponda.<br>– Generando registros de auditoría.<br>– Configurados para bloquear los ataques basados en la web o generar una alerta que se investigue inmediatamente.<br>– Funcionando activamente y actualizándose según corresponda.<br>– Generando registros de auditoría.<br>– Configurados para bloquear los ataques basados en la web o generar una alerta que se investigue inmediatamente. | | | | | | |
| | **Notas de Aplicabilidad**<br>Esta evaluación no es la misma que los escaneos de vulnerabilidad realizados para los Requisitos 11.3.1 y 11.3.2.<br>Este requisito será sustituido por el requisito 6.4.2 después del 31 de marzo de 2025, cuando entre en vigor el requisito 6.4.2. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.4.2** | Para aplicaciones web de cara al público se implementa una solución técnica automatizada que detecta e impide continuamente ataques basados en la web, con al menos lo siguiente:<br>• Se instala frente a aplicaciones web de cara al público y está configurado para detectar e impedir ataques basados en la web.<br>• Funcionando activamente y actualizándose según corresponda.<br>• Generando registros de auditoría.<br>• Configurados ya sea para bloquear los ataques basados en la web o para generar una alerta que se investigue inmediatamente. | • Evalúe los ajustes de configuración del sistema.<br>• Evalúe los registros de auditoría.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este nuevo requisito reemplazará al Requisito 6.4.1 una vez que termine su fecha de vigencia.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **6.4.3** | Todos los *scripts* de las páginas de pago que se cargan y ejecutan en el navegador del consumidor se gestionan de la siguiente manera: | | | | | | |
| | • Se implementa un método para confirmar que cada *script* está autorizado. | • Evalúe las políticas y procedimientos.<br>• Entreviste al personal responsable.<br>• Evalúe los registros de inventario.<br>• Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Se implementa un método para asegurar la integridad de cada *script*. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Se mantiene un inventario de todos los scripts con una justificación empresarial o técnica por escrito que explique su necesidad.<br>*(continuación)* | | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| | **Notas de Aplicabilidad** | | | | | | |
| | Este requisito se aplica a todos los scripts cargados desde el entorno de la entidad y a los scripts cargados desde terceras y cuartas partes.<br>Este requisito también se aplica a los scripts en la(s) página(s) web de la entidad que incluyen una página/formulario de pago incrustado de un TPSP/procesador de pagos (por ejemplo, uno o más marcos en línea o iframes).<br>Este requisito no se aplica a una entidad para scripts en una página/formulario de pago incrustado de un TPSP/procesador de pagos (por ejemplo, uno o más iframes), cuando la entidad incluye una página/formulario de pago del TPSP/procesador de pagos en su página web.<br>La gestión de los scripts en la página/formulario de pago incrustado del TPSP/procesador de pagos es responsabilidad del TPSP/procesador de pagos de acuerdo con este requisito.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **6.5** Los cambios en todos los componentes del sistema se gestionan de forma segura. | | | | | | | |
| **6.5.1** | Los cambios en todos los componentes del sistema en el entorno de producción se realizan de acuerdo con los procedimientos establecidos que incluyen:<br>• Motivo y descripción del cambio.<br>• Documentación del impacto a la seguridad.<br>• Aprobación documentada del cambio por las partes autorizadas.<br>• Pruebas para verificar que el cambio no afecta negativamente la seguridad del sistema.<br>• En el caso de los cambios de software a la medida y personalizados, todas las actualizaciones se comprueban para determinar que cumplen con el requisito 6.2.4 antes de ser instalados para producción.<br>• Procedimientos para hacer frente a los fallos y volver a un estado seguro. | • Evalúe los procedimientos documentados de control de cambios.<br>• Evalúe los cambios recientes a los componentes del sistema y rastree esos cambios hasta la documentación de control de cambios relacionada.<br>• Evalúe la documentación de control de cambios. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.5.2** | Al completar un cambio significativo, se confirma que todos los Requisitos de PCI DSS están vigentes en todos los sistemas y redes nuevos o modificados, y la documentación se actualiza según corresponda. | • Evalúe la documentación en busca de cambios significativos.<br>• Entreviste al personal.<br>• Observe los sistemas/redes afectados. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Estos cambios significativos también deben capturarse y reflejarse en la actividad de confirmación del alcance PCI DSS anual de la entidad, según el Requisito 12.5.2. | | | | | | |
| **6.5.3** | Los entornos de preproducción se separan de los entornos de producción y la separación se aplica con controles de acceso. | • Evalúe las políticas y procedimientos.<br>• Evalúe la documentación de la red y las configuraciones de los controles de seguridad de la red.<br>• Evalúe la configuración del control de acceso. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **6.5.4** | Los roles y las funciones se separan entre los entornos de producción y pre-producción para asignar responsabilidades de manera tal que sólo se desplieguen los cambios revisados y aprobados. | • Evalúe las políticas y procedimientos.<br>• Observe los procesos.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>En entornos con personal limitado donde los individuos desempeñan múltiples roles o funciones, este mismo objetivo puede lograrse con controles de procedimiento adicionales que asignen responsabilidades. Por ejemplo, un desarrollador puede ser también un administrador que utiliza una cuenta de nivel administrador con privilegios especiales en el entorno de desarrollo y, para su función de desarrollador, utiliza una cuenta separada con acceso de nivel de usuario al entorno de producción. | | | | | | |
| **6.5.5** | Los datos PAN activos no se utilizan en entornos de pre-producción, excepto cuando esos entornos están incluidos en el CDE y protegidos de acuerdo con todos los Requisitos de PCI DSS aplicable. | • Evalúe las políticas y procedimientos.<br>• Observe los procesos de prueba.<br>• Entreviste al personal.<br>• Evalúe los datos de las pruebas de preproducción. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **6.5.6** | Los datos de prueba y las cuentas de pruebas se eliminan de los componentes del sistema antes de que el sistema entre en producción. | • Evalúe las políticas y procedimientos.<br>• Observe los procesos de prueba tanto de los programas informáticos existentes como de las aplicaciones internas.<br>• Entreviste al personal.<br>• Evalúe los datos y las cuentas de los programas informáticos existentes actualizados y de las aplicaciones instaladas recientemente. | ☐ | ☐ | ☐ | ☐ | ☐ |

# Implementar Medidas Sólidas de Control de Acceso

## *Requisito 7: Restringir el Acceso a los Componentes del Sistema y a los Datos de Tarjetahabiente Según la Necesidad de Conocimiento de la Empresa*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **7.1** Se definen y comprenden los procesos y mecanismos para restringir el acceso a los componentes del sistema y a los datos de tarjetahabiente según la necesidad de negocio. | | | | | | | |
| **7.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 7 son:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 7 están documentadas, asignadas y son comprendidos. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2** El acceso a los componentes y datos del sistema se define y asigna adecuadamente. | | | | | | | |
| **7.2.1** | Se define un modelo de control de acceso que incluye la autorización de acceso como sigue:<br>• Acceso apropiado según el tipo de negocios de la entidad y las necesidades de acceso.<br>• Acceso a los componentes del sistema y a los recursos de datos basados en la clasificación y las funciones del trabajo del usuario.<br>• Los privilegios mínimos requeridos (por ejemplo, usuario, administrador) para realizar una función laboral. | • Evalúe las políticas y procedimientos documentados.<br>• Entreviste al personal.<br>• Evalúe la configuración del modelo de control de acceso. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **7.2.2** | El acceso se asigna a los usuarios, incluidos los privilegiados, en función de:<br>• La clasificación y función del trabajo.<br>• Los privilegios mínimos necesarios para realizar las responsabilidades del trabajo. | • Evalúe las políticas y procedimientos.<br>• Evalúe la configuración de acceso de los usuarios, incluso de los privilegiados.<br>• Entreviste al personal administrativo responsable.<br>• Entreviste al personal responsable de asignar el acceso. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.3** | Los privilegios requeridos son aprobados por el personal autorizado. | • Evalúe las políticas y procedimientos.<br>• Evalúe las identificaciones de los usuarios y los privilegios asignados.<br>• Evalúe las aprobaciones documentadas. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.2.4** | Todas las cuentas de usuario y los privilegios de acceso relacionados, incluyendo las cuentas de terceros/proveedores, se revisan de la siguiente manera:<br>• Al menos una vez cada seis meses.<br>• Para asegurarse de que las cuentas de usuario y el acceso sigan siendo apropiados según la función del trabajo.<br>• Se aborda cualquier acceso inadecuado.<br>• La gerencia reconoce que el acceso sigue siendo apropiado. | • Evalúe las políticas y procedimientos.<br>• Entreviste al personal responsable.<br>• Evalúe los resultados documentados de evaluaciones periódicas de las cuentas de usuarios. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito se aplica a todas las cuentas de usuario y privilegios de acceso relacionados incluyendo las que utiliza el personal y terceros/proveedores, y las cuentas utilizadas para acceder a servicios de terceros en la nube.<br><br>Consulte los Requisitos 7.2.5 y 7.2.5.1 y 8.6.1 a 8.6.3 para conocer los controles de aplicaciones y cuentas del sistema.<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **7.2.5** | Todas las aplicaciones y cuentas del sistema y los privilegios de acceso relacionados se asignan y administran de la siguiente manera:<br>• Basado en los privilegios mínimos necesarios para la operatividad del sistema o aplicación.<br>• El acceso está limitado a los sistemas, aplicaciones o procesos que específicamente requieren su uso. | • Evalúe las políticas y procedimientos.<br>• Evalúe los privilegios asociados a las cuentas del sistema y de las aplicaciones.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **7.2.5.1** | Todo el acceso de aplicaciones y cuentas del sistema y los privilegios de acceso relacionados se revisan de la siguiente manera:<br>• Periódicamente, (a una frecuencia definida en el análisis de riesgos específico de la entidad, el cual se desarrolla de acuerdo a todos los elementos especificados en el Requisito 12.3.1).<br>• El acceso a la aplicación/sistema sigue siendo apropiado para la función que se está realizando.<br>• Se aborda cualquier acceso inadecuado.<br>• La gerencia reconoce que el acceso sigue siendo apropiado. | • Evalúe las políticas y procedimientos.<br>• Evalúe el análisis de riesgos específico.<br>• Entreviste al personal responsable.<br>• Evalúe los resultados documentados de las revisiones periódicas de las cuentas del sistema y aplicaciones y de los privilegios correspondientes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **7.2.6** | Todo acceso por parte de los usuarios a las bases de datos de tarjetahabiente está restringido de la siguiente manera:<br>• A través de aplicaciones u otros métodos programáticos, con acceso y acciones permitidas basadas en las funciones y privilegios mínimos del usuario.<br>• Solo los administradores autorizados pueden acceder directamente o consultar las bases de datos de CHD almacenados. | • Evalúe las políticas y procedimientos.<br>• Entreviste al personal.<br>• Evalúe los ajustes de configuración para consultar los depósitos de datos de tarjetahabiente almacenados. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito se aplica a los controles para el acceso de los usuarios a las bases de datos de tarjetahabiente almacenados.<br><br>Consulte los Requisitos 7.2.5 y 7.2.5.1 y 8.6.1 a 8.6.3 para conocer los controles para aplicaciones y cuentas del sistema. | | | | | | |
| **7.3** El acceso a los componentes y datos del sistema se gestiona a través de un sistema de control de acceso. | | | | | | | |
| **7.3.1** | Existe un sistema de control de acceso que restringen el acceso según la necesidad del usuario y cubre todos los componentes del sistema. | • Evalúe la documentación del proveedor.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.3.2** | Los sistemas de control de acceso están configurados para aplicar los permisos asignados a individuos, aplicaciones, y sistemas basados en la clasificación y función del trabajo. | • Evalúe la documentación del proveedor.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **7.3.3** | El sistema de control de acceso está configurado para "denegar todo" predeterminadamente. | • Evalúe la documentación del proveedor.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |

## *Requisito 8: Identificar a los Usuarios y Autenticar el Acceso a los Componentes del Sistema*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.1** Los procesos y mecanismos para identificar a los usuarios y autenticar el acceso a los componentes del sistema están definidos y comprendidos. | | | | | | | |
| **8.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 8 están:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 8 están documentados, asignados y son comprendidos. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2** La identificación de usuarios y las cuentas relacionadas para usuarios y administradores se gestionan estrictamente durante el ciclo de vida de una cuenta. | | | | | | | |
| **8.2.1** | A todos los usuarios se les asigna un ID único antes de permitirles el acceso a los componentes del sistema o a los datos de tarjetahabiente. | • Entreviste al personal responsable.<br>• Evalúe los registros de auditoría y otras evidencias. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción. | | | | | | |

*Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.2.2** | Las identificaciones IDs de grupos, compartidas o genéricas, u otras credenciales de autenticación compartidas sólo se usan cuando es necesario, de manera excepcional, y se administran de la siguiente manera:<br>• Se impide el uso de la ID a menos que se requiera por una circunstancia excepcional.<br>• Su uso está limitado al tiempo necesario para la circunstancia excepcional.<br>• La justificación de negocio para su uso está documentada.<br>• Su uso está explícitamente aprobado por la dirección.<br>• La identidad del usuario individual se confirma antes de que se conceda el acceso a una cuenta.<br>• Cada acción realizada es atribuible a un usuario individual. | • Evalúe las listas de cuentas de usuario en los componentes del sistema y la documentación aplicable.<br>• Evalúe las políticas y procedimientos de autenticación.<br>• Entreviste a los administradores del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción. | | | | | | |
| **8.2.3** | ***Requisito adicional sólo para proveedores de servicios*** | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.2.4** | La creación, eliminación y modificación de IDs de usuario, factores de autenticación y otros objetos de identificación se gestiona de la siguiente manera:<br>• Autorizado con la aprobación correspondiente.<br>• Implementado solo con los privilegios especificados en la aprobación documentada. | • Evalúe las autorizaciones documentadas en las distintas fases del ciclo de vida de las cuentas (adiciones, modificaciones y bajas).<br>• Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito se aplica a todas las cuentas de usuario, incluyendo los empleados, contratistas, consultores, trabajadores temporales y proveedores externos. | | | | | | |
| **8.2.5** | El acceso para los usuarios que cesan se revoca inmediatamente. | • Evalúe las fuentes de información para los usuarios que han sido dados de baja.<br>• Revise las listas de acceso de los usuarios actuales.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.6** | Las cuentas de usuario inactivas se eliminan o inhabilitan dentro de los 90 días de inactividad. | • Evalúe las cuentas de usuario y la información del último inicio de sesión.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.2.7** | Las cuentas utilizadas por terceros para acceder, respaldar o mantener componentes del sistema a través de acceso remoto se administran de la siguiente manera:<br>• Son habilitadas solamente durante el período de tiempo necesario y son deshabilitadas cuando no están en uso.<br>• El uso es monitorizado para detectar cualquier actividad inesperada. | • Entreviste al personal responsable.<br>• Evalúe la documentación para la gestión de las cuentas.<br>• Evalúe la evidencia. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.2.8** | Si una sesión de usuario ha estado inactiva durante más de 15 minutos, se requiere que el usuario vuelva a autenticarse para reactivar el terminal o la sesión. | • Evalúe los ajustes de configuración del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción.<br>Este requisito no pretende impedir que se realicen actividades legítimas mientras la consola/PC está desatendida. | | | | | | |
| **8.3** Se establece y gestiona una autenticación robusta para usuarios y administradores. | | | | | | | |
| **8.3.1** | Todo acceso por parte de los usuarios y administradores a componentes del sistema se autentifica utilizando al menos uno de los siguientes factores de autenticación:<br>• Algo que uno sabe, como una contraseña o frase de paso.<br>• Algo que uno tiene, como un dispositivo token o una tarjeta inteligente.<br>• Algo que uno es, como un elemento biométrico. | • Evalúe la documentación que describe el factor o factores de autenticación utilizados.<br>• Para cada tipo de factor de autenticación utilizado con cada tipo de componente del sistema, observe el proceso de autenticación. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción.<br>Este requisito no sustituye a los requisitos de autenticación de múltiples factores (MFA), sino que se aplica a los sistemas incluidos en el ámbito de aplicación que no están sujetos a los requisitos de los MFA.<br>El certificado digital es una opción válida para "algo que se tiene" si es único para un usuario concreto. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.3.2** | Se utiliza criptografía robusta para que todos los factores de autenticación sean ilegibles durante la transmisión y el almacenamiento en todos los componentes del sistema. | • Evalúe la documentación del proveedor.<br>• Evalúe los ajustes de configuración del sistema.<br>• Evalúe los repositorios de factores de autenticación.<br>• Evalúe las transmisiones de datos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.3** | La identidad del usuario se verifica antes de modificar cualquier factor de autenticación. | • Evalúe los procedimientos para modificar los factores de autenticación.<br>• Observe al personal de seguridad. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **8.3.4** | Los intentos de autenticación inválidos se limitan mediante:<br>• El bloqueo del ID de usuario después de no más de 10 intentos.<br>• El establecimiento de la duración del bloqueo a un mínimo de 30 minutos o hasta que se confirme la identidad del usuario. | • Evalúe los ajustes de configuración del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción. | | | | | | |
| **8.3.5** | Si las contraseñas/frases de paso se utilizan como factores de autenticación para cumplir con el requisito 8.3.1, estas se establecen y restablecen para cada usuario tal y como sigue:<br>• Se establecen a un valor único para la primera vez que se utilizan y al restablecerse.<br>• Existe la obligatoriedad de cambiarlos inmediatamente después del primer uso. | • Evalúe los procedimientos para establecer y restablecer las contraseñas/frases de paso.<br>• Observe al personal de seguridad. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.3.6** | Si las contraseñas/frases de paso se utilizan como factores de autenticación para cumplir el requisito 8.3.1, estas deberán cumplir el siguiente nivel mínimo de complejidad:<br>• Una longitud mínima de 12 caracteres (o SI el sistema no admite 12 caracteres, una longitud mínima de ocho caracteres).<br>• Contener tanto caracteres numéricos como alfabéticos. | • Evalúe los ajustes de configuración del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito no se aplica a:<br>• Cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción.<br>• Cuentas de aplicaciones o sistemas, que se rigen por los requisitos de la sección 8.6.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual será obligatorio y debe tenerse en cuenta en su totalidad durante una evaluación PCI DSS.*<br>Hasta el 31 de marzo de 2025, las contraseñas deben tener una longitud mínima de siete caracteres, de acuerdo con el requisito 8.2.3 PCI DSS v3.2.1. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.3.7** | Las personas no pueden enviar una nueva contraseña / frase de paso que sea igual a cualquiera de las últimas cuatro contraseñas / frases de paso utilizadas. | • Evalúe los ajustes de configuración del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad** | | | | | | |
| | Este requisito no está destinado a aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta simultáneamente para procesar una única transacción. | | | | | | |
| **8.3.8** | Las políticas y los procedimientos de autenticación están documentados y son comunicados a todos los usuarios, incluyendo:<br>• Orientación sobre la selección de factores de autenticación robustos.<br>• Orientación sobre cómo los usuarios deben proteger sus factores de autenticación.<br>• Instrucciones para no reutilizar contraseñas/frases de paso utilizadas anteriormente.<br>• Instrucciones para cambiar contraseñas/frases de paso si existe alguna sospecha o conocimiento de que la contraseña/frase de paso se ha visto comprometida y cómo reportar el incidente. | • Evalúe los procedimientos.<br>• Entreviste al personal.<br>• Revise las políticas y procedimientos de autenticación que se distribuyen a los usuarios.<br>• Entreviste a los usuarios. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.3.9** | Si las contraseñas/frases de paso se utilizan como el único factor de autenticación para el acceso del usuario (es decir, en cualquier implementación de autenticación de factor único), entonces:<br>• Las contraseñas/frases de paso se cambian al menos una vez cada 90 días,<br>**O**<br>• La postura de seguridad de las cuentas se analiza dinámicamente y el acceso a los recursos en tiempo real se determina automáticamente de acuerdo a dicha postura de seguridad. | • Inspeccione los ajustes de configuración del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br>Este requisito no se aplica a los componentes del sistema incluidos en el ámbito de aplicación en los que se utilice MFA.<br>Este requisito no se aplica a las cuentas de usuarios de terminales de puntos de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.<br>Este requisito no se aplica a las cuentas de clientes de proveedores de servicios, pero se aplica a las cuentas del personal del proveedor de servicios. | | | | | | |
| **8.3.10** | ***Requisito adicional sólo para proveedores de servicios*** | | | | | | |
| **8.3.10.1** | ***Requisito adicional sólo para proveedores de servicios*** | | | | | | |
| **8.3.11** | Cuando se utilizan factores de autenticación como *tokens* de seguridad físicos o lógicos, tarjetas inteligentes o certificados:<br>• Los factores se asignan a un usuario individual y no se comparten entre varios usuarios.<br>• Los controles físicos y/o lógicos garantizan que sólo el usuario previsto pueda utilizar ese factor para acceder. | • Evalúe las políticas y procedimientos de autenticación.<br>• Entreviste al personal de seguridad.<br>• Evalúe los ajustes de configuración del sistema y/o observe los controles físicos, según corresponda. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.4** Se implementa la autenticación múltiples factores (MFA) para proteger el ingreso al CDE. | | | | | | | |
| **8.4.1** | Los MFA se implementan para todos los accesos al CDE sin consola, para el personal con acceso administrativo. | • Evalúe las configuraciones de la red y/o del sistema.<br>• Observe al personal de administración que se registra en el CDE. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El requisito de MFA para el acceso administrativo sin consola se aplica a todo el personal con privilegios elevados o aumentados que accede al CDE a través de una conexión sin consola, es decir, a través de un acceso lógico que se produce a través de una interfaz de red en lugar de una conexión directa y física. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.4.2** | Los MFA se implementan para todos los accesos sin consola al CDE. | • Evalúe las configuraciones de la red y/o del sistema.<br>• Observe al personal que se registra en el CDE.<br>• Evalúe la evidencia. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad** | | | | | | |
| | Este requisito no se aplica a:<br>• Aplicación o cuentas del sistema que desempeñan funciones automatizadas.<br>• Cuentas de usuario en terminales de punto de venta que tienen acceso a un solo número de tarjeta a la vez para facilitar una sola transacción.<br>• Cuentas de usuario que sólo se autentican con factores de autenticación resistentes al phishing.<br>Se requieren los MFA para ambos tipos de accesos especificados en los Requisitos 8.4.2 y 8.4.3. Por lo tanto, la aplicación de los MFA a un tipo de acceso no reemplaza la necesidad de aplicar otra instancia de MFA al otro tipo de acceso. Si una persona se conecta primero a la red de la entidad a través de un acceso remoto, y luego inicia una conexión al CDE desde dentro de la red; según este requisito, la persona se autenticaría usando los MFA dos veces, una cuando se conecta a través de acceso remoto a la red de la entidad, y luego cuando se conecta a través de un acceso de la entidad al CDE.<br>Los requisitos de los MFA se aplican a todos los tipos de componentes del sistema, incluyendo la nube, los sistemas alojados y las aplicaciones locales, los dispositivos de seguridad de red, las estaciones de trabajo, los servidores y los puntos finales, e incluye el acceso directo a las redes o sistemas de una entidad, así como el acceso basado en web a una aplicación o función.<br>Los MFA para ingreso al CDE se pueden implementar a nivel de red o sistema/aplicación; no es necesario que se apliquen en ambos niveles. Por ejemplo, si se usan MFA cuando un usuario se conecta a la red del CDE, no es necesario que se usen cuando el usuario inicia sesión en cada sistema o aplicación dentro del CDE.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.4.3** | Los MFA se implementan para todos los accesos a redes remotas que se originan fuera de la red de la entidad y que podrían ingresar o impactar el CDE. | • Evalúe las configuraciones de la red y/o del sistema para los servidores y sistemas de acceso remoto.<br>• Observe al personal (por ejemplo, usuarios y administradores) y terceros que se conecta de forma remota a la red. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El requisito de los MFA para el acceso remoto que se origina desde fuera de la red de la entidad se aplica a todas las cuentas de usuario que pueden ingresar a la red de forma remota, donde ese acceso remoto conduce o podría conducir a un acceso al CDE. Esto incluye todos los accesos remotos del personal (usuarios y administradores) y los terceros (incluidos, entre otros, los vendedores, proveedores de servicios y clientes).<br><br>Si el acceso remoto se realiza a una parte de la red de la entidad que está correctamente segmentada del CDE, de manera que los usuarios remotos no puedan ingresar al CDE o afectarlo, no se requiere MFA para el acceso remoto a esa parte de la red. Sin embargo, se requieren los MFA para cualquier acceso remoto a redes con acceso al CDE y se recomienda para todos los accesos remotos a las redes de la entidad.<br><br>Los requisitos de los MFA se aplican a todos los tipos de componentes del sistema, incluyendo la nube, los sistemas alojados y las aplicaciones locales, los dispositivos de seguridad de red, las estaciones de trabajo, los servidores y los puntos finales, e incluye el acceso directo a las redes o sistemas de una entidad, así como el acceso basado en web a una aplicación o función. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.5** Los sistemas de autenticación de múltiples factores (MFA) están configurados para evitar su uso indebido. | | | | | | | |
| **8.5.1** | Los sistemas MFA se implementan de la siguiente manera:<br>• El sistema MFA no es susceptible a ataques de repetición.<br>• Los sistemas MFA no pueden ser omitidos por ningún usuario, incluyendo los usuarios administrativos, a menos que esté específicamente documentado y autorizado por la administración de manera excepcional durante un período de tiempo limitado.<br>• Se utilizan al menos dos tipos diferentes de factores de autenticación.<br>• Se requiere el éxito de todos los factores de autenticación antes de que se otorgue el acceso.<br>**Notas de Aplicabilidad**<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | • Evalúe la documentación del sistema del proveedor.<br>• Evalúe las configuraciones del sistema para la aplicación de la MFA.<br>• Entreviste al personal responsable y observe los procesos.<br>• Observe al personal que se conecta a los componentes del sistema en el CDE.<br>• Observe al personal conectándose de forma remota desde fuera de la red de la entidad. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.6** El uso de cuentas de aplicaciones y sistemas y factores de autenticación asociados se gestiona estrictamente. | | | | | | | |
| **8.6.1** | Si las cuentas utilizadas por los sistemas o aplicaciones pueden ser utilizadas para el inicio de sesión interactivo, se gestionan de la siguiente manera:<br>• Se impide el uso interactivo a menos que se requiera por una circunstancia excepcional.<br>• El uso está limitado al tiempo necesario para la circunstancia excepcional.<br>• La justificación de negocio para su uso está documentada.<br>• El uso interactivo está explícitamente aprobado por la dirección.<br>• La identidad del usuario individual se confirma antes de que se conceda el acceso a una cuenta.<br>• Cada acción realizada es atribuible a un usuario individual. | • Evalúe las cuentas de las aplicaciones y del sistema que se pueden utilizar para inicio de sesión interactivo.<br>• Entreviste al personal administrativo. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.6.2** | Las contraseñas/frases de paso para cualquier aplicación y cuentas de sistema que puedan ser utilizadas para el inicio de sesión interactivo no están codificadas en scripts, archivos de configuración/propiedades, o código fuente a la medida y personalizado. | • Entreviste al personal.<br>• Evalúe los procedimientos de desarrollo del sistema.<br>• Evalúe los *scripts*, archivos de configuración/propiedades, y el código fuente personalizado y a la medida para las cuentas de aplicación y sistema que pueden ser utilizadas para iniciar sesiones interactivas. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad** | | | | | | |
| | Las contraseñas/frases de acceso almacenadas deben estar cifradas de acuerdo con el Requisito 8.3.2 PCI DSS.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **8.6.3** | Las contraseñas/frases de paso para cualquier cuenta de aplicación y de sistema están protegidas contra el uso indebido de la siguiente manera:<br>• Las cuentas de sistema y de aplicación se cambian periódicamente, (a una frecuencia definida en el análisis de riesgos específico de la entidad, el cual se desarrolla de acuerdo a todos los elementos especificados en el Requisito 12.3.1.) y ante la sospecha o la confirmación de que estén comprometidas.<br>• Las contraseñas/frases de acceso se construyen con la complejidad necesaria y apropiada para la frecuencia con la que la entidad cambia las contraseñas/frases de acceso. | • Evalúe las políticas y procedimientos.<br>• Evalúe el análisis de riesgos específico.<br>• Entreviste al personal responsable.<br>• Evalúe los ajustes de configuración del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

## *Requisito 9: Restringir el Acceso Físico a los Datos de Tarjetahabiente*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.1** Se definen y comprenden los procesos y mecanismos para restringir el ingreso físico a los datos de tarjetahabiente. | | | | | | | |
| **9.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 9 están:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 9 están documentadas, asignadas y comprendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.2** Los controles de ingreso físico gestionan la entrada a las instalaciones y sistemas que contengan datos de tarjetahabiente. | | | | | | | |
| **9.2.1** | Existen controles de entrada a las instalaciones apropiados para restringir el ingreso físico a los sistemas en el CDE.<br>**Notas de Aplicabilidad**<br>Este requisito no se aplica a los lugares que son de acceso público para los consumidores (tarjetahabientes). | • Observe los controles físicos de entrada.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.2.1.1** | El acceso físico individual a las áreas sensibles dentro del CDE se monitoriza con cámaras de video vigilancia o mecanismos de control de acceso físico (o ambos) como sigue:<br>• Los puntos de entrada y salida hacia/desde las áreas sensibles dentro del CDE son monitorizados.<br>• Los dispositivos o mecanismos de monitorización están protegidos contra la manipulación o la desactivación.<br>• Los datos recogidos se revisan y se correlacionan con otras entradas.<br>• Los datos recogidos se almacenan durante al menos tres meses, a menos que la ley lo restrinja. | • Observe las locaciones donde se produce el acceso físico de individuos a las áreas sensibles dentro del CDE.<br>• Observe los mecanismos de control de acceso físico y/o examine las cámaras de vídeo.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.2.2** | Se implementan controles físicos y/o lógicos para restringir el uso de tomas (o puertos) de red de acceso público dentro de la instalación. | • Entreviste al personal responsable.<br>• Observe la ubicación de los conectores de red de acceso público. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.2.3** | El acceso físico a los puntos de acceso inalámbricos, puertas de enlace (gateways), hardware de redes y de comunicaciones y líneas de telecomunicaciones dentro de la instalación está restringido. | • Entreviste al personal responsable.<br>• Observe la ubicación del hardware y de las líneas. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.2.4** | El acceso a las consolas en áreas sensibles está restringido mediante bloqueo cuando no están en uso. | • Observe el intento de un administrador de sistemas de ingresar a las consolas en áreas sensibles. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.3** Se autoriza y gestiona el acceso físico de personal y visitantes. | | | | | | | |
| **9.3.1** | Se implementan procedimientos para autorizar y administrar el acceso físico del personal al CDE, que incluyen:<br>• Identificación de personal.<br>• Gestionar cambios en los requisitos de acceso físico de una persona.<br>• Revocación o rescisión de la identificación del personal.<br>• Limitar el acceso al proceso o sistema de identificación al personal autorizado. | • Evalúe los procedimientos documentados.<br>• Observar los métodos de identificación, como las tarjetas de identificación.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.3.1.1** | El acceso físico a áreas sensibles dentro del CDE para el personal se controla de la siguiente manera:<br>• El acceso está autorizado y se basa en la función del trabajo individual.<br>• El acceso se revoca inmediatamente después de la terminación.<br>• Todos los mecanismos de acceso físico, como llaves, tarjetas de acceso, etc., se devuelven o desactivan al finalizar. | • Observe al personal en las zonas sensibles del CDE.<br>• Entreviste al personal responsable.<br>• Observe la lista control de ingreso físico.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.3.2** | Se implementan procedimientos para autorizar y administrar el acceso de visitantes al CDE, que incluyen:<br>• Los visitantes son autorizados antes de ingresar.<br>• Los visitantes están acompañados en todo momento.<br>• Los visitantes están claramente identificados y reciben un gafete u otra identificación con fecha de caducidad.<br>• Los gafetes de visitante u otra identificación distinguen visiblemente a los visitantes del personal. | • Evalúe los procedimientos documentados.<br>• Observe los procesos cuando los visitantes están presentes ene l CDE.<br>• Entreviste al personal.<br>• Observe el uso de gafetes de visitante u otra identificación. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.3.3** | Los gafetes de visitante o la identificación se devuelven o desactivan antes de que los visitantes abandonen las instalaciones, o en su fecha de caducidad. | • Observe a los visitantes abandonando las instalaciones.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.3.4** | Los registros de visitantes se utilizan para mantener un registro físico de las actividades de los visitantes tanto dentro de la instalación como en las áreas sensibles, que incluye:<br>• El nombre del visitante y la organización representada.<br>• La fecha y hora de la visita.<br>• El nombre del personal que autoriza el acceso físico.<br>• Los datos recogidos se almacenan durante al menos tres meses, a menos que la ley lo restrinja. | • Evalúe los registros de visitantes.<br>• Entreviste al personal responsable.<br>• Evalúe las ubicaciones de almacenamiento del registro de visitantes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4** Los medios con datos de tarjetahabiente se almacenan, acceden, distribuyen y destruyen de forma segura. | | | | | | | |
| **9.4.1** | Todos los medios que contienen datos de tarjetahabiente están protegidos físicamente. | • Evalúe la documentación. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.1.1** | Las copias de seguridad sin conexión con los datos de tarjetahabiente se almacenan en una ubicación segura. | • Evalúe los procedimientos documentados.<br>• Evalúe los registros u otra documentación.<br>• Entreviste al personal responsable de en el sitio de almacenamiento. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.1.2** | La protección de las ubicaciones de las copias de seguridad fuera de línea que contienen los datos de tarjetahabiente, se revisa al menos una vez cada 12 meses. | • Evalúe los procedimientos documentados, los registros u otra documentación.<br>• Entreviste al personal responsable de en el sitio de almacenamiento. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.4.2** | Todos los datos de tarjetahabiente se clasifican de acuerdo con la confidencialidad de esos datos. | • Evalúe los procedimientos documentados.<br>• Evalúe los registros en medios u otra documentación. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.3** | Los apoyos con datos de tarjetahabiente enviados fuera de las instalaciones se protegen de la siguiente manera:<br>• Los datos enviados fuera de las instalaciones se registran.<br>• Los datos se envían por mensajería segura u otro método de entrega que pueda ser rastreado con precisión.<br>• Los registros de seguimiento fuera de las instalaciones incluyen detalles sobre la ubicación de los datos. | • Evalúe los procedimientos documentados.<br>• Entreviste al personal.<br>• Evalúe los registros.<br>• Evalúe los registros de seguimiento externo de todos los medios. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.4.4** | La gerencia aprueba todos los movimientos de apoyos con datos de tarjetahabiente que se trasladan fuera de las instalaciones (incluso cuando son distribuidos a particulares). | • Evalúe los procedimientos documentados.<br>• Evalúe los registros de seguimiento externo.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Las personas que aprueban los movimientos de los apoyos deben tener el nivel adecuado de autoridad de gestión para conceder esta aprobación. Sin embargo, no se requiere específicamente que dichas personas tengan el título de "gerente". | | | | | | |
| **9.4.5** | Se mantienen registros de inventario de todos los apoyos electrónicos con datos de tarjetahabiente. | • Evalúe los procedimientos documentados.<br>• Evalúe los registros del inventario de medios electrónicos.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.4.5.1** | Los inventarios de apoyos electrónicos con datos de tarjetahabiente se realizan al menos una vez cada 12 meses. | • Evalúe los procedimientos documentados.<br>• Evalúe los registros del inventario de medios electrónicos.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.4.6** | Los materiales impresos con datos de tarjetahabiente se destruyen cuando ya no se necesitan por razones de negocios o legales, de la siguiente manera:<br>• Los materiales se trituran transversalmente, se incineran o se pulverizan de forma que los datos de tarjetahabiente no puedan reconstruirse.<br>• Los materiales se guardan en contenedores de almacenamiento seguro antes de su destrucción. | • Evalúe la política de destrucción de medios.<br>• Observe los procesos.<br>• Entreviste al personal.<br>• Observe los contenedores de almacenamiento. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Estos requisitos relativos a la destrucción de materiales impresos cuando éstos ya no son necesarios por motivos de negocio o legales son independientes y distintos del requisito 3.2.1 PCI DSS, que se refiere a la eliminación segura de los datos de tarjetahabiente cuando ya no son necesarios de acuerdo con las políticas de retención de datos de tarjetahabiente de la entidad. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.4.7** | Los medios de almacenamiento electrónicos con datos de tarjetahabiente se destruyen cuando ya no se necesitan por razones de negocio o legales mediante una de las siguientes opciones:<br>• El medio de almacenamiento electrónico se destruye.<br>• Los datos de tarjetahabiente se vuelven irrecuperables, de modo que no pueden reconstruirse. | • Evalúe la política de destrucción de medios.<br>• Observe el proceso de destrucción de medios.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Estos requisitos relativos a la destrucción de medios de almacenamiento cuando éstos ya no son necesarios por motivos de negocio o legales son independientes y distintos del requisito 3.2.1 PCI DSS, que se refiere a la eliminación segura de los datos de tarjetahabiente cuando ya no son necesarios de acuerdo con las políticas de retención de datos de tarjetahabiente de la entidad. | | | | | | |
| **9.5** Los dispositivos de Punto de Interacción (POI) están protegidos contra alteraciones y sustituciones no autorizadas. | | | | | | | |
| **9.5.1** | Los dispositivos POI que capturan los datos de los tarjetahabientes a través de la interacción física directa con el factor de forma de la tarjeta de pago están protegidos contra la manipulación y la sustitución no autorizada, incluyendo lo siguiente:<br>• Mantener una lista de dispositivos de POI.<br>• Inspeccionar periódicamente los dispositivos POI en busca de manipulaciones o sustituciones no autorizadas.<br>• Formar al personal para que esté atento a los comportamientos sospechosos y denuncie las manipulaciones o sustituciones no autorizadas de los dispositivos.<br>*(continuación)* | • Evalúe las políticas y procedimientos documentados. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| | **Notas de Aplicabilidad**<br><br>Estos requisitos se aplican a los dispositivos de POI desplegados que se utilizan en transacciones con tarjeta física (es decir, un factor de forma de tarjeta de pago como una tarjeta que se pasa, se toca o se introduce).<br>Estos requisitos no se aplican a:<br>• Componentes utilizados únicamente para la introducción manual de claves PAN.<br>• Dispositivos comerciales listos para usar (*commercial off-the-shelf*, COTS) (por ejemplo, teléfonos inteligentes o tabletas), que son dispositivos móviles propiedad del comerciante diseñados para la distribución masiva. | | | | | | |
| **9.5.1.1** | Se mantiene una lista actualizada de los dispositivos POI, incluyendo:<br>• Marca y modelo del dispositivo.<br>• Ubicación del dispositivo.<br>• Número de serie del dispositivo u otros métodos de identificación única. | • Evalúe la lista de dispositivos POI.<br>• Observe los dispositivos POI y la ubicación de los dispositivos.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.5.1.2** | Las superficies de los dispositivos POI se inspeccionan periódicamente para detectar manipulaciones y sustituciones no autorizadas. | • Evalúe los procedimientos documentados.<br>• Entreviste al personal responsable.<br>• Observe los procesos de inspección. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **9.5.1.2.1** | La frecuencia de las inspecciones a los dispositivos POI y el tipo de inspección que se realice se define en el análisis de riesgos específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1. | • Evalúe el análisis de riesgos específico.<br>• Evalúe los resultados documentados de las revisiones de registros.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **9.5.1.3** | Se proporciona capacitación para que el personal en entornos POI esté al tanto de los intentos de manipulación o reemplazo de dispositivos POI, lo que incluye:<br>• Verificar la identidad de cualquier tercero que afirme ser personal de reparación o mantenimiento, antes de otorgarles acceso para modificar o solucionar problemas en los dispositivos.<br>• Procedimientos para garantizar que los dispositivos no se instalen, reemplacen o devuelvan sin verificación.<br>• Ser consciente de comportamientos sospechosos alrededor de los dispositivos.<br>• Informar sobre comportamientos sospechosos e indicaciones de manipulación o sustitución de dispositivos al personal apropiado. | • Revisar los materiales de capacitación del personal en entornos POI.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

# Monitorear y Verificar las Redes Regularmente

## *Requisito 10: Registrar y Supervisar Todos los Accesos a los Componentes del Sistema y a los Datos de Tarjetahabiente*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **10.1** Se definen y entienden los procesos y mecanismos para ingresar y monitorear todos los accesos a los componentes del sistema y a los datos de tarjetahabiente. | | | | | | | |
| **10.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 10 están:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 10 están documentadas, asignadas y comprendidas. | • Evalúe la documentación<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2** Los registros de auditoría se implementan para respaldar la detección de anomalías y actividades sospechosas, y el análisis forense de eventos. | | | | | | | |
| **10.2.1** | Los registros de auditoría están habilitados y activos para todos los componentes del sistema y los datos de tarjetahabiente. | • Entreviste a los administradores del sistema.<br>• Evalúe las configuraciones del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1.1** | Los registros de auditoría capturan todo el acceso de los usuarios individuales a los datos de tarjetahabiente. | • Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **10.2.1.2** | Los registros de auditoría almacenan todas las acciones realizadas por cualquier individuo con acceso administrativo, incluyendo cualquier uso interactivo de la aplicación o cuentas del sistema. | • Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1.3** | Los registros de auditoría capturan todo el acceso a los mismos. | • Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1.4** | Los registros de auditoría capturan todos los intentos de acceso lógico inválidos. | • Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1.5** | Los registros de auditoría capturan todos los cambios en la identificación y credenciales de autenticación, lo que incluye, entre otros:<br>• Creación de nuevas cuentas.<br>• Elevación de privilegios.<br>• Todos los cambios, adiciones o eliminaciones de cuentas con acceso administrativo. | • Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1.6** | Los registros de auditoría capturan lo siguiente:<br>• Toda inicialización de nuevos registros de auditoría y<br>• Todo inicio, la detención o la pausa de los registros de auditoría existentes. | • Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.2.1.7** | Los registros de auditoría capturan toda la creación y eliminación de objetos a nivel del sistema. | • Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **10.2.2** | Los registros de auditoría guardan los siguientes detalles para cada evento auditable:<br>• Identificación del usuario.<br>• Tipo de evento.<br>• Fecha y hora.<br>• Indicación de Exitoso o Fallido.<br>• Origen del evento.<br>• Identidad o nombre de los datos, componentes del sistema, recursos o servicios afectados (por ejemplo, nombre y protocolo). | • Entreviste al personal responsable.<br>• Evalúe las configuraciones del registro de auditoría.<br>• Evalúe los datos de registros de auditoría. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3** Los registros de auditoría están protegidos contra la destrucción y las modificaciones no autorizadas. | | | | | | | |
| **10.3.1** | El acceso de lectura a los archivos de registros de auditoría está limitado a aquellos con una necesidad relacionada con sus funciones. | • Entreviste a los administradores del sistema.<br>• Evalúe las configuraciones del sistema y los privilegios. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.2** | Los archivos de registros de auditoría están protegidos para evitar modificaciones por parte de terceros. | • Evalúe las configuraciones del sistema y los privilegios.<br>• Entreviste a los administradores del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.3** | Los archivos de registros de auditoría, incluidos los de tecnologías externas, se respaldan con prontitud en un servidor de registro interno seguro, central o sobre otro medio que sea difícil de modificar. | • Evalúe las configuraciones de las copias de seguridad o los archivos de registro. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.3.4** | Los mecanismos de detección de cambios o supervisión de la integridad de los archivos se utilizan en registros de auditoría para garantizar que los datos de registros existentes no se puedan modificar sin generar alertas. | • Evalúe las configuraciones del sistema.<br>• Evalúe los archivos monitoreados.<br>• Evalúe los resultados de las actividades de monitoreo. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **10.4** Los registros de auditoría se revisan para identificar anomalías o actividades sospechosas. | | | | | | | |
| **10.4.1** | Los siguientes registros de auditoría se revisan al menos una vez al día:<br>• Todos los eventos de seguridad.<br>• Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD.<br>• Registros de todos los componentes críticos del sistema.<br>• Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, controles de seguridad de red, sistemas de detección de intrusiones/sistemas de prevención de intrusiones (IDS / IPS), servidores de autenticación). | • Evalúe las políticas y procedimientos de seguridad.<br>• Observe los procesos.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.4.1.1** | Se utilizan mecanismos automatizados para realizar revisiones de los registros de auditoría.<br>**Notas de Aplicabilidad**<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | • Evalúe los mecanismos de revisión de los registros.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **10.4.2** | Los registros de todos los demás componentes del sistema (aquellos no especificados en el Requisito 10.4.1) se revisan periódicamente. | • Evalúe las políticas y procedimientos de seguridad.<br>• Evalúe los resultados documentados de las revisiones de los registros.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito es aplicable a todos los demás componentes del sistema dentro del alcance no incluidos en el Requisito 10.4.1. | | | | | | |
| **10.4.2.1** | La frecuencia de las evaluaciones periódicas de los componentes del sistema identificados (No definidos en el Requisito 10.4.1) se define en el análisis de riesgo específico de la entidad, el cual se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1 | • Evalúe el análisis de riesgos específico.<br>• Evalúe los resultados documentados de las revisiones de registros periódicas.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **10.4.3** | Se abordan las excepciones y anomalías identificadas durante el proceso de revisión. | • Evalúe las políticas y procedimientos de seguridad.<br>• Observe los procesos.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.5** Se conserva el historial del registro de auditoría y está disponible para su análisis. | | | | | | | |
| **10.5.1** | Conserve el historial de los registros de auditoría por 12 meses como mínimo, teniendo al menos los tres últimos meses inmediatamente disponibles para su análisis. | • Evalúe las políticas y procedimientos documentados de conservación de registros de auditoría.<br>• Evalúe las configuraciones del historial del registro de auditoría.<br>• Evalúe los registros de auditoría.<br>• Entreviste al personal.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **10.6** Los mecanismos de sincronización de la hora admiten una configuración de hora coherente en todos los sistemas. | | | | | | | |
| **10.6.1** | Los relojes del sistema y la hora están sincronizados usando tecnología de sincronización de tiempo.<br><br>**Notas de Aplicabilidad**<br><br>Mantener actualizada la tecnología de sincronización horaria incluye la aplicación de parches como lo establecen los Requisitos 6.3.1 y 6.3.3 PCI DSS. | • Evalúe los ajustes de configuración del sistema. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.6.2** | Los sistemas están configurados con la hora correcta y consistente como sigue:<br>• Uno o más servidores de tiempo designados están en uso.<br>• Solo los servidores de hora central designados reciben la hora de fuentes externas.<br>• La hora recibida de fuentes externas se basa en la Hora Atómica Internacional u Hora Universal Coordinada (UTC).<br>• Los servidores de tiempo designados aceptan actualizaciones de tiempo solo de fuentes externas específicas aceptadas por la industria.<br>• Cuando hay más de un servidor de tiempo designado, los servidores de tiempo se emparejan entre sí para mantener la hora exacta.<br>• Los sistemas internos reciben información de la hora solo de los servidores de hora central designados. | • Evalúe los ajustes de configuración del sistema para adquirir, distribuir y almacenar la hora correcta. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **10.6.3** | La configuración de sincronización de la hora y los datos están protegidos de la siguiente manera:<br>• El acceso a los datos de tiempo está restringido solo al personal con una necesidad de negocio.<br>• Cualquier cambio en la configuración de tiempo en sistemas críticos se registra, monitorea y verifica. | • Evalúe las configuraciones del sistema y los ajustes y registros de sincronización horaria.<br>• Observe los procesos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **10.7** Las fallas de los sistemas de control de seguridad críticos se detectan, informan y atienden con prontitud. | | | | | | | |
| **10.7.1** | ***Requisito adicional sólo para proveedores de servicios*** | | | | | | |
| **10.7.2** | Las fallas de los sistemas de control de seguridad críticos se detectan, alertan y abordan con prontitud, incluyendo entre otras, las fallas de los siguientes sistemas de control de seguridad críticos:<br>• Controles de seguridad de la red.<br>• IDS/IPS.<br>• Cambiar los mecanismos de detección.<br>• Soluciones antimalware.<br>• Controles de acceso físico.<br>• Controles de Ingreso lógico.<br>• Mecanismos de registro de auditoría.<br>• Controles de segmentación (si se utilizan).<br>• Mecanismos de revisión del registro de auditoría.<br>• Herramientas de prueba de seguridad automatizadas (si se utilizan).<br>*(continuación)* | • Evalúe los procesos documentados.<br>• Observar los procesos de detección y alertas.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| | **Notas de Aplicabilidad**<br><br>Este requisito se aplica a todas las entidades, incluidos los proveedores de servicios, y sustituirá al requisito 10.7.1 a partir del 31 de marzo de 2025. Incluye dos sistemas de control de seguridad críticos adicionales que no aparecen en el Requisito 10.7.1.<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **10.7.3** | Las fallas de cualquier sistema de control de seguridad crítico se responden con prontitud, incluidas, entre otras, las siguientes:<br>• Restaurando las funciones de seguridad.<br>• Identificando y documentando la duración (fecha y hora de principio a fin) de la falla de seguridad.<br>• Identificando y documentando las causas de las fallas y documentando el remedio requerido.<br>• Identificando y abordando cualquier problema de seguridad que surgió durante la falla.<br>• Determinar si se requieren más acciones como resultado de la falla de seguridad.<br>• Implementar controles para evitar que se repita la causa de la falla.<br>• Reanudación del monitoreo de los controles de seguridad.<br>*(continuación)* | • Evalúe los procesos documentados.<br>• Entreviste al personal.<br>• Evalúe los registros relacionados con los fallos de los sistemas de control de seguridad críticos. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|
| | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **Notas de Aplicabilidad**<br><br>Este requisito se aplica únicamente cuando la entidad evaluada es un proveedor de servicios hasta el 31 de marzo de 2025, fecha a partir de la cual este requisito se aplicará a todas las entidades.<br>*Este es un requisito actual de la versión 3.2.1 que aplica solo a los proveedores de servicios. Sin embargo, este requisito es una práctica recomendada para todas las demás entidades hasta el 31 de marzo de 2025, después de lo cual será obligatoria y debe considerarse en su totalidad durante una evaluación PCI DSS.* | | | | | | |

## *Requisito 11: Poner a Prueba Regularmente la Seguridad de los Sistemas y de las Redes*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.1** Se definen y comprenden los procesos y mecanismos para probar periódicamente la seguridad de los sistemas y redes. | | | | | | | |
| **11.1.1** | Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 11 son:<br>• Documentados.<br>• Actualizados.<br>• En uso.<br>• Conocidos por todas las partes involucradas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.1.2** | Los roles y responsabilidades para realizar las actividades del Requisito 11 son documentadas, asignadas y entendidas. | • Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.2** Se identifican y controlan los puntos de acceso inalámbricos y se abordan los puntos de acceso inalámbricos no autorizados. | | | | | | | |
| **11.2.1** | Los puntos de acceso inalámbricos autorizados y no autorizados se gestionan de la siguiente manera:<br>• Se comprueba la existencia de puntos de acceso inalámbricos (Wi-Fi) para,<br>• Detectar e identificar todos los puntos de acceso inalámbricos autorizados y no autorizados,<br>• Que la verificación, detección e identificación ocurre al menos cada tres meses.<br>• Si se utiliza la supervisión automatizada, se notifica al personal mediante la generación de alertas. | • Evalúe las políticas y procedimientos.<br>• Evalúe las metodologías utilizadas y la documentación resultante.<br>• Entreviste al personal<br>• Evalúe los resultados de la evaluación inalámbrica.<br>• Evalúe los ajustes de configuración. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito aplica incluso cuando existe una política que prohíbe el uso de la tecnología inalámbrica.<br><br>Los métodos utilizados para cumplir este requisito deben ser suficientes para detectar e identificar tanto los dispositivos autorizados como los no autorizados, incluidos los dispositivos no autorizados conectados a dispositivos que sí están autorizados. | | | | | | |
| **11.2.2** | Se mantiene un inventario de los puntos de acceso inalámbricos autorizados, incluyendo una justificación de negocio documentada. | • Evalúe la documentación. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.3** Las vulnerabilidades externas e internas se identifican, se priorizan y se abordan periódicamente. | | | | | | | |
| **11.3.1** | Los escaneos de vulnerabilidades internas se realizan de la siguiente manera:<br>• Al menos una vez cada tres meses.<br>• Se resuelven las vulnerabilidades de alto riesgo o críticas (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1).<br>• Se realizan re-escaneos que confirman que se han resuelto todas las vulnerabilidades críticas y de alto riesgo (como se indicó anteriormente).<br>• La herramienta de escaneo se mantiene actualizada con la información más reciente sobre vulnerabilidades.<br>• Los escaneos son realizados por personal calificado con la independencia organizacional del probador. | • Evalúe los resultados del informe de escaneo interno.<br>• Evalúe las configuraciones de las herramientas de escaneo.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>No es necesario utilizar un QSA o un ASV para realizar escaneos internos de vulnerabilidades.<br><br>Los escaneos de vulnerabilidades internas pueden ser realizados por personal interno calificado que sea razonablemente independiente de los componentes del sistema que se analizan (por ejemplo, un administrador de red no debería ser responsable de analizar la red), o una entidad puede optar por una empresa especializada en escaneos de vulnerabilidades. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.3.1.1** | Todas las demás vulnerabilidades aplicables (aquellas que no se clasifican como vulnerabilidades de alto riesgo o vulnerabilidades críticas según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1) se gestionan de la siguiente manera:<br>• Abordado en función del riesgo definido en el análisis de riesgo específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el Requisito 12.3.1.<br>• Los re-escaneos se realizan según sea necesario. | • Evalúe el análisis de riesgos específico.<br>• Entreviste al personal responsable.<br>• Evalúe los resultados del informe de escaneo interno y otra documentación. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El plazo para abordar las vulnerabilidades de menor riesgo está sujeto a los resultados de un análisis de riesgo según el Requisito 12.3.1 que incluye (mínimamente) la identificación de los activos que se protegen, las amenazas y la probabilidad y / o el impacto de una amenaza que se realiza.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.3.1.2** | Los escaneos de vulnerabilidades internas se realizan mediante escaneos autenticados como sigue: | | | | | | |
| | • Se documentan los sistemas que no pueden aceptar credenciales para el escaneo autenticado. | • Evalúe la documentación.<br>• Evalúe las configuraciones de las herramientas de escaneo.<br>• Evalúe los resultados del informe de escaneo.<br>• Entreviste al personal.<br>• Evalúe las cuentas utilizadas para el escaneo autentificado. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Se utilizan suficientes privilegios para aquellos sistemas que aceptan credenciales para escanear. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Si las cuentas utilizadas para el escaneo autenticado se pueden utilizar para el inicio de sesión interactivo, estas se gestionan de acuerdo con el Requisito 8.2.2 | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Las herramientas de escaneo autenticadas pueden estar basadas en *host* o en red.<br><br>Los privilegios "suficientes" son los necesarios para ingresar a los recursos del sistema, de modo que se pueda realizar un análisis exhaustivo que detecte vulnerabilidades conocidas.<br><br>Este requisito no se aplica a los componentes del sistema que no pueden aceptar credenciales para escanear. Algunos ejemplos de sistemas que pueden no aceptar credenciales para escanear incluyen algunos dispositivos de red y seguridad, servidores y contenedores.<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.3.1.3** | Los escaneos internos de vulnerabilidades se realizan después de cualquier cambio significativo como sigue:<br>• Se resuelven las vulnerabilidades que son de alto riesgo o críticas (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1).<br>• Los re-escaneos se realizan según sea necesario.<br>• Los escaneos son realizados por personal cualificado con la independencia organizacional del probador (no se requiere que sea un QSA o ASV). | • Evalúe la documentación de control de cambios.<br>• Entreviste al personal.<br>• Evalúe los informes de escaneo y re-escaneo cuando sea aplicable.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>No se requiere el escaneo de vulnerabilidades internas autenticado según el Requisito 11.3.1.2 para los análisis realizados después de cambios significativos. | | | | | | |
| **11.3.2** | Los escaneos externos de vulnerabilidad se realizan de la siguiente manera:<br>• Al menos una vez cada tres meses.<br>• Por parte de un proveedor de Escaneo Aprobado por PCI SSC (ASV).<br>• Las vulnerabilidades se resuelven y se cumple con los requisitos de la *Guía del Programa* ASV.<br>• Se realizan nuevos escaneos según sea necesario para confirmar que las vulnerabilidades se han resuelto de acuerdo con los requisitos de la *Guía del Programa* ASV escaneos aprobados.<br>*(continuación)* | • Evalúe los reportes de escaneos ASV. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| | **Notas de Aplicabilidad**<br><br>Para la evaluación inicial de PCI DSS con respecto a este requisito, no es necesario que se completen cuatro escaneos aprobados en un plazo de 12 meses si el asesor verifica que: 1) el resultado del escaneo más reciente fue un escaneo satisfactorio, 2) la entidad ha documentado políticas y procedimientos que requieren escaneos al menos una vez cada tres meses, y 3) las vulnerabilidades observadas en los resultados del escaneo se han corregido como se muestra en un re-escaneo.<br><br>Sin embargo, durante los años siguientes después de la evaluación inicial PCI DSS, deben haberse realizado escaneos aprobados al menos cada tres meses.<br><br>Las herramientas de escaneo de ASV pueden escanear una amplia gama de tipos y topologías de redes. Cualquier detalle sobre el entorno de destino (por ejemplo, distribuidores de carga, proveedores externos, ISP, configuraciones específicas, protocolos en uso, interferencia de escaneo) debe resolverse entre el ASV y el cliente de escaneo.<br><br>Consulte la *Guía del Programa* ASV publicada en el sitio web PCI SCC para conocer las responsabilidades del cliente de escaneo, la preparación del escaneo, etc. | | | | | | |
| **11.3.2.1** | Los escaneos externos se realizan después de cualquier cambio significativo de la siguiente manera:<br>• Se resuelven las vulnerabilidades calificadas con 4.0 o más por CVSS.<br>• Los re-escaneos se realizan según sea necesario.<br>• Los escaneos son realizados por personal calificado con la independencia organizacional del probador (no se requiere que sea un QSA o ASV). | • Evalúe la documentación de control de cambios.<br>• Entreviste al personal<br>• Evalúe los informes de escaneo externo y, en su caso, los informes de re-escaneo. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.4** Las pruebas de penetración externas e internas se realizan con regularidad y se corrigen las vulnerabilidades explotables y las debilidades de seguridad. | | | | | | | |
| **11.4.1** | La entidad define, documenta e implementa una metodología de prueba de penetración, que incluye:<br>• Enfoques de pruebas de penetración aceptados por la industria.<br>• Cobertura para todo el perímetro de CDE y sus sistemas críticos.<br>• Pruebas tanto dentro como fuera de la red.<br>• Pruebas para validar cualquier control de segmentación y reducción del alcance.<br>• Pruebas de penetración a nivel de la aplicación para identificar, como mínimo, las vulnerabilidades enumeradas en el Requisito 6.2.4.<br>• Las pruebas de penetración a nivel de red que abarcan todos los componentes que admiten las funciones de red y los sistemas operativos.<br>• Revisión y consideración de amenazas y vulnerabilidades experimentadas en los últimos 12 meses.<br>• Enfoque documentado para evaluar y abordar el riesgo que plantean las vulnerabilidades explotables y las debilidades de seguridad encontradas durante las pruebas de penetración.<br>• Retención de los resultados de las pruebas de penetración y los resultados de las actividades de remediación durante al menos 12 meses.<br>*(continuación)* | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| | **Notas de Aplicabilidad**<br><br>Realizar pruebas desde el interior de la red (o "pruebas de penetración interna") significa realizar pruebas tanto desde el interior del CDE como hacia el CDE proviniendo de redes internas confiables y no confiables.<br><br>Pruebas desde fuera de la red (o pruebas de penetración "externas") significa probar el perímetro externo expuesto de redes confiables y sistemas críticos conectado o accesible a infraestructuras de redes públicas. | | | | | | |
| **11.4.2** | Se realizan pruebas de penetración interna:<br>• Según la metodología definida por la entidad,<br>• Al menos una vez cada 12 meses.<br>• Después de cualquier actualización o cambio significativo de infraestructura o aplicación<br>• Por un recurso interno calificado o un tercero externo calificado<br>• El asesor cuenta con independencia organizacional (no se requiere que sea un QSA o ASV). | • Evalúe el ámbito de trabajo.<br>• Evalúe los resultados de la prueba de penetración externa más reciente.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.4.3** | Se realizan pruebas de penetración externa:<br>• Según la metodología definida por la entidad<br>• Al menos una vez cada 12 meses<br>• Después de cualquier actualización o cambio significativo de infraestructura o aplicación<br>• Por un recurso interno calificado o un tercero externo calificado<br>• El asesor cuenta con independencia organizacional (no se requiere que sea un QSA o ASV). | • Evalúe el ámbito de trabajo.<br>• Evalúe los resultados de la prueba de penetración externa más reciente.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.4.4** | Las vulnerabilidades explotables y las debilidades de seguridad encontradas durante las pruebas de penetración se corrigen de la siguiente manera:<br>• De acuerdo con la evaluación de la entidad, del riesgo que representa el problema de seguridad según se define en el Requisito 6.3.1.<br>• La prueba de penetración se repite para verificar las correcciones. | • Evalúe los resultados de la prueba de penetración. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.4.5** | Si la segmentación se utiliza para aislar el CDE de otras redes, las pruebas de penetración se realizan en los controles de segmentación de la siguiente manera:<br>• Al menos una vez cada 12 meses y después de cualquier cambio en los controles/métodos de segmentación.<br>• Cubriendo todos los controles/métodos de segmentación en uso.<br>• De acuerdo con la metodología de prueba de penetración definida por la entidad.<br>• Confirmar que los controles/métodos de segmentación son operativos y eficientes, y aislar al CDE de todos los sistemas fuera del ámbito.<br>• Confirmar la efectividad de cualquier uso de aislamiento para separar sistemas con diferentes niveles de seguridad (ver Requisito 2.2.3).<br>• Realizado por un recurso interno calificado o un tercero externo calificado.<br>• El asesor cuenta con independencia organizacional (no se requiere que sea un QSA o ASV). | • Evalúe los controles de segmentación.<br>• Revise la metodología de penetración-prueba.<br>• Evalúe los resultados de la prueba de penetración más reciente.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta* (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **11.4.6** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **11.4.7** | ***Requisito adicional sólo para proveedores de servicios multiusuario.*** | | | | | | |
| **11.5** Las intrusiones de red y los cambios inesperados de archivos se detectan y se responden. | | | | | | | |
| **11.5.1** | Las técnicas de detección y/o prevención de intrusiones se utilizan para detectar y/o impedir intrusiones en la red de la siguiente manera:<br>• Todo el tráfico se supervisa en el perímetro del CDE.<br>• Todo el tráfico se supervisa en los puntos críticos del CDE.<br>• Se envía una alerta al personal indicando las sospechas de situaciones comprometidas.<br>• Todos los motores de detección y prevención de intrusiones, las líneas de base y las firmas se mantienen actualizadas. | • Evalúe las configuraciones del sistema y los diagramas de red.<br>• Evalúe las configuraciones del sistema.<br>• Entreviste al personal responsable.<br>• Evalúe la documentación del proveedor. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **11.5.1.1** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **11.5.2** | Un mecanismo de detección de cambios (por ejemplo, herramientas de monitoreo de integridad de archivos) se despliega como sigue:<br>• Para alertar al personal sobre modificaciones no autorizadas (incluyendo cambios, adiciones y eliminaciones) de archivos críticos.<br>• Para realizar comparaciones de archivos críticos al menos una vez por semana. | • Evalúe la configuración del sistema para el mecanismo de detección de cambios.<br>• Evalúe los archivos monitoreados.<br>• Evalúe los resultados de las actividades de monitoreo. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| | **Notas de Aplicabilidad** | | | | | | |
| | A efectos de detección de cambios, los archivos críticos suelen ser aquellos que no cambian regularmente, pero cuya modificación podría indicar poner en riesgo el sistema o comprometerlo. Los mecanismos de detección de cambios, como los productos de monitoreo de la integridad de los archivos, suelen venir pre-configurados con archivos críticos para el sistema operativo correspondiente. Otros archivos críticos, como los de las aplicaciones personalizadas, deben ser evaluados y definidos por la entidad (es decir, el comerciante o proveedor de servicios). | | | | | | |
| **11.6** Se detectan los cambios no autorizados en las páginas de pago y se responden. | | | | | | | |
| **11.6.1** | El mecanismo de detección de cambios y manipulaciones se despliega de la siguiente manera: | | | | | | |
| | • Para enviar alertas al personal sobre modificaciones no autorizadas (incluyendo indicadores de situaciones comprometidas, cambios, adiciones y supresiones) en los encabezados HTTP que afectan la seguridad y en el contenido de *script* de las páginas de pago tal y como las recibe el navegador del consumidor. | • Evalúe los ajustes del sistema y la configuración del mecanismo.<br>• Evalúe las páginas de pago monitoreadas.<br>• Evalúe los resultados de las actividades de monitoreo.<br>• Evalúe los ajustes de configuración del mecanismo.<br>• Evalúe los ajustes de configuración.<br>• Entreviste al personal responsable.<br>• Si aplica, evalúe el análisis de riesgos específico. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • El mecanismo está configurado para evaluar el encabezamiento HTTP y la página de pago recibidas.<br>*(continuación)* | | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|
| | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| • Las funciones del mecanismo se realizan de la siguiente manera:<br>– Al menos semanalmente<br>**O**<br>– Periódicamente, (a una frecuencia definida en el análisis de riesgos específico de la entidad, el cual se desarrolla de acuerdo a todos los elementos especificados en el Requisito 12.3.1.) | | | | | | |
| **Notas de Aplicabilidad**<br><br>Este requisito también se aplica a las entidades con una(s) página(s) web que incluyen una página/formulario de pago incrustado de un TPSP/procesador de pagos (por ejemplo, uno o más marcos en línea o iframes).<br><br>Este requisito no se aplica a una entidad para scripts en una página/formulario de pago incrustado de un TPSP/procesador de pagos (por ejemplo, uno o más iframes), cuando la entidad incluye una página/formulario de pago del TPSP/procesador de pagos en su sitio web.<br><br>La gestión de los scripts en la página/formulario de pago incrustado del TPSP/procesador de pagos es responsabilidad del TPSP/procesador de pagos de acuerdo con este requisito.<br><br>La intención de este requisito no es que una entidad necesite instalar software en los sistemas o navegadores de sus consumidores, sino que la entidad utilice técnicas como las descritas en los ejemplos anteriores para detectar e impedir actividades inesperadas de scripts.<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

# Mantener una Política de Seguridad de la Informática

## *Requisito 12: Respaldar la Seguridad de la Información con Políticas y Programas Organizacionales*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.1** Una política integral de seguridad de la información que rija y proporcione orientación para la protección de los activos de información de la entidad es actualizada y bien conocida. | | | | | | | |
| **12.1.1** | Una política general de seguridad de la información es:<br>• Establecida.<br>• Publicada.<br>• Mantenida.<br>• Difundida a todo el personal relevante, así como a los proveedores y socios comerciales relevantes. | • Evalúe la política de protección informática.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1.2** | La política de seguridad de la información es:<br>• Revisada al menos una vez cada 12 meses.<br>• Actualizada según sea necesario para reflejar los cambios en los objetivos de negocios o los riesgos para el entorno. | • Evalúe la política de protección informática.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1.3** | La política de seguridad define claramente los roles y responsabilidades de seguridad de la información para todo el personal, y todo el personal conoce y reconoce sus responsabilidades en materia de seguridad de la información. | • Evalúe la política de protección informática.<br>• Entreviste al personal responsable.<br>• Evalúe las evidencias documentadas. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.1.4** | La responsabilidad de la seguridad de la información se asigna formalmente a un director de seguridad de la información o a otro miembro de la dirección ejecutiva con conocimientos de seguridad de la información. | • Evalúe la política de protección informática. | ☐ | ☐ | ☐ | ☐ | ☐ |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.2** Se definen e implementan políticas de uso aceptable para tecnologías de usuario final. | | | | | | | |
| **12.2.1** | Se documentan e implementan políticas de uso aceptable para tecnologías orientadas al usuario final, que incluyen:<br>• Aprobación explícita por las partes autorizadas.<br>• Usos aceptables de la tecnología.<br>• Lista de productos aprobados por la empresa para uso de los empleados, incluidos hardware y software. | • Evalúe las políticas de uso aceptables.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Ejemplos de tecnologías orientadas al usuario final para las que se espera sean aplicadas políticas de uso aceptable son, entre otras, tecnologías inalámbricas y de acceso remoto, computadoras portátiles, tabletas, teléfonos móviles y medios electrónicos extraíbles, uso del correo electrónico y uso de Internet. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.3** Los riesgos para el entorno de datos de tarjetahabiente se identifican, evalúan y gestionan formalmente. | | | | | | | |
| **12.3.1** | Para cada requisito de PCI DSS que especifique completar un análisis de riesgo específico, el análisis se documenta e incluye:<br>• Identificación de los activos a proteger.<br>• Identificación de las amenazas contra las que protege el requisito.<br>• Identificación de factores que contribuyen a la probabilidad y/o impacto de que se materialice una amenaza.<br>• Análisis resultante que determine e incluya la justificación de, cómo la frecuencia o los procesos definidos por la entidad para cumplir el requisito minimizan la probabilidad y/o el impacto de que se materialice la amenaza.<br>• Revisión de cada análisis de riesgo específico al menos una vez cada 12 meses para determinar si los resultados siguen siendo válidos o si se necesita un análisis de riesgo actualizado.<br>• Realización de análisis de riesgos actualizados cuando sea necesario, según lo determinado por la revisión anual.<br>**Notas de Aplicabilidad**<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | • Evalúe las políticas y procedimientos documentados. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.3.2** | ***Este requisito es específico del enfoque personalizado y no se aplica a las entidades que rellenan un cuestionario de autoevaluación.*** | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.3.3** | Los protocolos y conjuntos de cifrado criptográfico en uso se documentan y revisan al menos una vez cada 12 meses, incluyendo al menos lo siguiente:<br>• Un inventario actualizado de todos los protocolos y conjuntos de cifrado criptográfico en uso, incluyendo su propósito y dónde se utilizan.<br>• Monitoreo activo de las tendencias de la industria con respecto a la viabilidad continua de todos los protocolos y conjuntos de cifrado criptográfico en uso.<br>• Documentación de un plan para responder a los cambios anticipados en las vulnerabilidades criptográficas. | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El requisito requisito se aplica a todos los conjuntos y protocolos criptográficos utilizados para cumplir con los requisitos de PCI DSS, incluidos, entre otros, los utilizados para hacer que el PAN sea ilegible en el almacenamiento y la transmisión, para proteger las contraseñas y como parte de la autenticación del acceso.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.3.4** | Las tecnologías de hardware y software en uso se revisan al menos una vez cada 12 meses, incluyendo al menos lo siguiente:<br>• Análisis de que las tecnologías continúan recibiendo correcciones de seguridad por parte de los proveedores con prontitud.<br>• Análisis de que las tecnologías continúan apoyando (y no imposibilitan) el cumplimiento PCI DSS de la entidad.<br>• Documentación de cualquier anuncio o tendencia de la industria relacionada con una tecnología, como cuando un proveedor ha anunciado planes para el "fin de la vida útil" de una tecnología.<br>• Documentación de un plan, aprobado por la alta gerencia, para remediar tecnologías obsoletas, incluidas aquellas para las que los proveedores han anunciado planes de "fin de vida útil". | • Evalúe la documentación.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **12.4** Gestión del cumplimiento con PCI DSS. | | | | | | | |
| **12.4.1** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **12.4.2** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **12.4.2.1** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.5** Documentación y validación del alcance PCI DSS. | | | | | | | |
| **12.5.1** | Se mantiene y actualiza un inventario de los componentes del sistema que están dentro del alcance PCI DSS, incluyendo una descripción de su función/uso. | • Evalúe el inventario.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.5.2** | El alcance PCI DSS es documentado y confirmado por la entidad al menos una vez cada 12 meses y ante cambios significativos en el entorno dentro del alcance. | • Evalúe los resultados documentados de las revisiones dl alcance.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | ***Como mínimo, la validación del alcance incluye:*** | | | | | | |
| | • Identificar todos los flujos de datos para las diversas etapas de pago (por ejemplo, autorización, captura de la liquidación, devoluciones y reembolsos) y canales de aceptación (por ejemplo, tarjeta física, tarjeta virtual y comercio electrónico). | • Evalúe los resultados documentados de las revisiones dl alcance. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Actualizar todos los diagramas de flujo de datos según el Requisito 1.2.4. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Identificar todas las ubicaciones donde se almacenan, procesan y transmiten datos del titular de la tarjeta, incluidos, entre otros: 1) cualquier ubicación fuera del CDE definida actualmente, 2) aplicaciones que procesan CHD, 3) transmisiones entre sistemas y redes, y 4) copias de seguridad de archivos. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Identificar todos los componentes del sistema en el CDE, conectados al CDE o que podrían afectar la seguridad del CDE.<br>*(continuación)* | | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| | • Identificar todos los controles de segmentación en uso y los entornos desde los que se segmenta el CDE, incluida la justificación de los entornos que están fuera del alcance. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Identificar todas las conexiones de entidades de terceros con acceso al CDE. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | • Confirmar que todos los flujos de datos identificados, datos del titular de la tarjeta, componentes del sistema, controles de segmentación y conexiones de terceros con acceso al CDE están incluidos en el alcance. | | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Se espera que esta confirmación anual del alcance PCI DSS sea una actividad realizada por la entidad que se está evaluando, y no es la misma, ni pretende ser reemplazada por, la confirmación del alcance realizada por el asesor de la entidad durante la evaluación anual. | | | | | | |
| **12.5.2.1** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **12.5.3** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **12.6** La educación en concienciación sobre la seguridad es una actividad continua. | | | | | | | |
| **12.6.1** | Se implementa un programa formal de concientización sobre seguridad para que todo el personal conozca la política y los procedimientos de seguridad de la información a de la entidad, y el rol del personal en la protección de los datos de tarjetahabiente. | • Evalúe el programa de concienciación sobre seguridad. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.6.2** | El programa de concientización sobre seguridad es:<br>• Revisado al menos una vez cada 12 meses, y<br>• Actualizado según sea necesario para abordar cualquier nueva amenaza y vulnerabilidad que pueda afectar la seguridad de datos de tarjetahabiente y/o datos de autenticación sensibles de la entidad, o la información proporcionada al personal sobre sus funciones en lo concerniente a la protección de los datos de tarjetahabiente.<br>**Notas de Aplicabilidad**<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | • Evalúe el programa de concienciación sobre seguridad.<br>• Evalúe las revisiones de evidencias.<br>• Entreviste al personal. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.6.3** | El personal recibe capacitación sobre seguridad de la siguiente manera:<br>• Al momento de la contratación y al menos una vez cada 12 meses.<br>• A través de múltiples métodos de comunicación.<br>• El personal reconoce al menos una vez cada 12 meses que ha leído y comprendido las políticas y los procedimientos de seguridad de la información. | • Evalúe los registros del programa de concienciación sobre seguridad.<br>• Entreviste al personal aplicable.<br>• Evalúe los materiales del programa de concienciación sobre seguridad.<br>• Evalúe el reconocimiento del personal. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.6.3.1** | El entrenamiento de concientización de seguridad incluye la concientización ante amenazas y vulnerabilidades que podrían impactar la seguridad los datos de tarjetahabiente o datos de autenticación sensibles, incluyendo, pero no limitado a:<br>• *Phishing* y ataques relacionados.<br>• Ingeniería social. | • Evalúe el contenido de la capacitación en concienciación sobre la seguridad. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Véase el requisito 5.4.1 para obtener orientación sobre la diferencia entre los controles técnicos y automatizados para detectar y proteger a los usuarios de los ataques de phishing y este requisito, para proporcionar a los usuarios capacitación en concientización sobre seguridad en materia de suplantación de identidad e ingeniería social. Se trata de dos requisitos distintos y separados, y uno de ellos no se cumple aplicando los controles exigidos por el otro.<br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |
| **12.6.3.2** | La capacitación en concientización sobre seguridad incluye la concientización sobre el uso aceptable de las tecnologías de usuario final de acuerdo con el requisito 12.2.1. | • Evalúe el contenido de la capacitación en concienciación sobre la seguridad. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.7** El personal es evaluado para reducir los riesgos de amenazas internas. | | | | | | | |
| **12.7.1** | El personal potencial que tendrá acceso al CDE es investigado, en el marco de las limitaciones que establecen las leyes locales, antes de su contratación, a fin de minimizar el riesgo de ataques provenientes de fuentes internas. | • Entreviste al personal directivo responsable del departamento de Recursos Humanos. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Para el personal potencial que vaya a ser contratado para puestos como los de cajeros en tiendas, que sólo tienen acceso a un número de tarjeta a la vez cuando facilitan una transacción, este requisito es sólo una recomendación. | | | | | | |
| **12.8** Gestión del riesgo de los activos de información asociados a las relaciones con proveedores de servicios externos (TPSP). | | | | | | | |
| **12.8.1** | Se mantiene una lista de todos los proveedores de servicios de terceros (TPSP) con los que se comparten datos del titular de la tarjeta o que podrían afectar a la seguridad de los datos del titular de la tarjeta, incluyendo una descripción para cada uno de los servicios prestados. | • Evalúe las políticas y procedimientos.<br>• Evalúe la lista de TPSP. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>El uso de un TPSP que cumpla con PCI DSS no hace que una entidad esté en cumplimiento con PCI DSS, ni elimina la responsabilidad de la entidad por su propio cumplimiento PCI DSS. | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.8.2** | Se mantienen acuerdos escritos con los TPSP de la siguiente manera:<br>• Se mantienen acuerdos escritos con todos los TPSP con los que se comparten datos del titular de la tarjeta o que podrían afectar la seguridad del CDE.<br>• Los acuerdos escritos incluyen el reconocimiento por parte de los TPSP de que los TPSP son responsables por la seguridad de los datos del titular de la tarjeta que los TPSP poseen o almacenan, procesan o transmiten en nombre de la entidad, o en la medida en que puedan afectar a la seguridad de los datos tarjetahabiente o datos de autenticación sensibles de la entidad. | • Evalúe las políticas y procedimientos.<br>• Evalúe los acuerdos escritos con los TPSP. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>La redacción exacta de un acuerdo dependerá de los detalles del servicio que se esté proporcionando y de las responsabilidades asignadas a cada parte. El acuerdo no tiene que incluir la redacción exacta proporcionado en este requisito.<br><br>El reconocimiento por escrito del TPSP es una confirmación que establece que el TPSP es responsable de la seguridad de los datos de cuenta que pueda almacenar, procesar o transmitir en nombre del cliente o en la medida en que el TPSP pueda afectar la seguridad de los datos tarjetahabiente o datos de autenticación sensibles<br><br>La evidencia de que un TPSP cumple con los requisitos de PCI DSS no es lo mismo que el reconocimiento por escrito especificado en este requisito. Por ejemplo, una Certificación de Cumplimiento (AOC) de PCI DSS, una declaración en el sitio web de una empresa, una declaración de políticas, una matriz de responsabilidades u otra evidencia que no esté incluida en un acuerdo escrito no es un reconocimiento por escrito. | | | | | | |
| **12.8.3** | Se implementa un proceso establecido para contratar a los TPSP, incluyendo la debida diligencia antes de la contratación. | • Evalúe las políticas y procedimientos.<br>• Evalúe la evidencia.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ (Marque una respuesta para cada requisito) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.8.4** | Se implementa un programa para monitorear el estado de conformidad PCI DSS de los TPSP al menos una vez cada 12 meses. | • Evalúe las políticas y procedimientos.<br>• Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Cuando una entidad tiene un acuerdo con un TPSP para cumplir con los requisitos de PCI DSS en nombre de la entidad (por ejemplo, a través de un servicio de *firewall*), la entidad debe trabajar con el TPSP para asegurarse de que se cumplan los requisitos de PCI DSS aplicables. Si el TPSP no cumple con los requisitos de PCI DSS aplicables, entonces, esos requisitos tampoco "están implementados" para la entidad. | | | | | | |
| **12.8.5** | Se mantiene información sobre qué requisitos de PCI DSS gestiona cada TPSP, cuáles gestiona la entidad y cualquiera que se comparta entre el TPSP y la entidad. | • Evalúe las políticas y procedimientos.<br>• Evalúe la documentación.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.9** Los proveedores de servicios externos (TPSP) respaldan la conformidad con los PCI DSS de sus clientes. | | | | | | | |
| **12.9.1** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **12.9.2** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.10** Respuesta inmediata a incidentes de seguridad sospechosos y confirmados que podrían afectar al CDE. | | | | | | | |
| **12.10.1** | Existe un plan de respuesta a incidentes y está listo para activarse en caso de sospecha o confirmación de un incidente de seguridad. El plan incluye, pero no se limita a:<br>• Funciones, responsabilidades y estrategias de comunicación y contacto en caso de sospecha o confirmación de un incidente de seguridad, incluyendo la notificación de marcas de pago y adquirentes, como mínimo.<br>• Procedimientos de respuesta a incidentes con actividades específicas de contención y mitigación para diferentes tipos de incidentes.<br>• Procedimientos de recuperación y continuidad del negocio.<br>• Procesos de apoyo de datos.<br>• Análisis de requisitos legales para reportar situaciones comprometidas.<br>• Cobertura y respuestas de todos los componentes críticos del sistema.<br>• Referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago. | • Evalúe el plan de respuesta a incidentes.<br>• Entreviste al personal.<br>• Evalúe la documentación de los incidentes reportados anteriormente. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.2** | Al menos una vez cada 12 meses, el plan de respuesta a incidentes de seguridad es:<br>• Revisado y el contenido actualizado según sea necesario.<br>• Probado, incluyendo todos los elementos enumerados en el Requisito 12.10.1. | • Entreviste al personal.<br>• Evalúe la documentación. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.3** | Se designa personal específico para estar disponible las 24 horas del día, los 7 días de la semana a fin de responder a incidentes de seguridad sospechosos o confirmados. | • Entreviste al personal responsable.<br>• Evalúe la documentación. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.10.4** | El personal responsable de responder a incidentes de seguridad sospechados y confirmados recibe capacitación adecuada y periódica sobre sus responsabilidades en la respuesta a incidentes. | • Entreviste al personal responsable por incidentes.<br>• Evalúe la documentación de capacitación. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **12.10.4.1** | La frecuencia de la capacitación periódica del personal de respuesta a incidentes es definida según el análisis de riesgos específico de la entidad, que se realiza de acuerdo con todos los elementos especificados en el requisito 12.3.1. | • Evalúe el análisis de riesgos específico. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.10.5** | El plan de respuesta a incidentes de seguridad incluye el monitoreo y la respuesta a las alertas de los sistemas de monitoreo de seguridad, incluyendo, pero no limitado a:<br>• Sistemas de detección y prevención de intrusiones.<br>• Controles de seguridad de la red.<br>• Mecanismos de detección de cambios en archivos críticos.<br>• El mecanismo de detección de cambios y manipulaciones en las páginas de pago. *Este punto es una de las mejores prácticas hasta su fecha de vigencia; consulte las Notas de Aplicabilidad que aparecen a continuación para obtener más detalles.*<br>• Detección de puntos de acceso inalámbricos no autorizados. | • Evalúe la documentación.<br>• Observe los procesos de respuesta a incidentes. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*El punto anterior (para supervisar y responder a las alertas de un mecanismo de detección de cambios y manipulaciones para las páginas de pago) es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual se exigirá como parte del requisito 12.10.5 y deberá tenerse plenamente en cuenta durante una evaluación PCI DSS.* | | | | | | |
| **12.10.6** | El plan de respuesta a incidentes de seguridad se modifica y evoluciona de acuerdo con las lecciones aprendidas y para incorporar los desarrollos de la industria. | • Evalúe las políticas y procedimientos.<br>• Evalúe el plan de seguridad de respuesta a incidentes.<br>• Entreviste al personal responsable. | ☐ | ☐ | ☐ | ☐ | ☐ |

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **12.10.7** | Existen procedimientos de respuesta a incidentes que se iniciarán cuando se detecten datos de PAN almacenados en un lugar inesperado, e incluyen:<br>• Determinar qué hacer si se descubren datos de PAN fuera del CDE, incluyendo su recuperación, eliminación segura y/o migración al CDE actualmente definido, según corresponda.<br>• Identificar si los datos de autenticación sensibles se almacenan con datos de PAN.<br>• Determinar de dónde proceden los datos del titular de la tarjeta y cómo han llegaron donde no se esperaba.<br>• Remediar fugas de datos o brechas en el proceso que llevaron a que los datos del titular de la tarjeta llegaran a una ubicación inesperada. | • Evaluar los procedimientos de respuesta a incidentes que estén documentados.<br>• Entreviste al personal.<br>• Evaluar los registros de acciones de respuesta. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>*Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, fecha a partir de la cual será obligatorio y deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.* | | | | | | |

# Anexo A: Requisitos Adicionales de PCI DSS

## *Anexo A1: Requisitos Adicionales de PCI DSS para Proveedores de Servicios Multiusuario*

Este Anexo no se utiliza para las evaluaciones comerciales.

## *Anexo A2: Requisitos Adicionales PCI DSS Para Entidades que Utilizan SSL /Primeras Versiones de TLS para Conexiones de Terminal POS POI Presencial con Tarjetas*

| Requisito de PCI DSS | | Pruebas Previstas | Respuesta♦ *(Marque una respuesta para cada requisito)* | | | | |
|---|---|---|---|---|---|---|---|
| | | | Implementado | Implementado con CCW | No Aplicable | No Probado | No Implementado |
| **A2.1** Los terminales POI que utilizan SSL y/o versiones iniciales de TLS no son susceptibles a vulnerabilidades conocidas de SSL/TLS. | | | | | | | |
| **A2.1.1** | Cuando los terminales POS POI del comerciante o en la ubicación de aceptación de pagos usan SSL y/o primeras versiones de, la entidad confirma que los dispositivos no son susceptibles a ninguna vulnerabilidad conocida para esos protocolos. | • Evalúe la documentación (por ejemplo, documentación del proveedor, detalles de la configuración del sistema o de la red) que verifica que los dispositivos no son susceptibles a vulnerabilidades conocidas para SSL/TLS inicial. | ☐ | ☐ | ☐ | ☐ | ☐ |
| | **Notas de Aplicabilidad**<br><br>Este requisito está destinado a aplicarse a la entidad con el terminal POS POI, como un comerciante. Este requisito no está destinado a los proveedores de servicios que sirven como punto de terminación o conexión a esos terminales POS POI. Los requisitos A2.1.2 y A2.1.3 se aplican a los proveedores de servicios POS POI.<br><br>La asignación para terminales POS POI que actualmente no son susceptibles a vulnerabilidades se basa en los riesgos actualmente conocidos. Si se introducen nuevas vulnerabilidades a las que los terminales POS POI son susceptibles, estas deberán actualizarse inmediatamente. | | | | | | |
| **A2.1.2** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |
| **A2.1.3** | ***Requisito adicional sólo para proveedores de servicios.*** | | | | | | |

♦ *Consulte la sección "Respuestas a los Requisitos" (página vi) para obtener información sobre estas opciones de respuesta.*

## *Anexo A3: Validación Complementaria de Entidades Designadas (DESV)*

Este Anexo se aplica solo a las entidades designadas por una marca de pago o adquirente que requieren una validación adicional de los Requisitos de PCI DSS vigentes. Las entidades que deban validar este Anexo deben utilizar la Plantilla de Informes Complementarios DESV y la Certificación de Conformidad complementaria para la presentación de informes y consultar con la marca de pago y/o el adquirente correspondiente para los procedimientos de presentación.

# Anexo B: Ficha de Control Compensatorio

*Este Anexo debe llenarse para definir los controles compensatorios para cualquier requisito en el que se haya seleccionado Implementado con CCW.*

***Nota:** Sólo las entidades que tengan limitaciones tecnológicas o comerciales legítimas y documentadas pueden considerar el uso de controles compensatorios para lograr la conformidad.*

*Refiérase a los Anexos B y C del PCI DSS para más información acerca de los controles compensatorios y orientación sobre cómo llenar esta hoja.*

**Número de Requisito y Definición:**

| | Información Requerida | Explicación |
|---|---|---|
| **1. Restricciones** | Documente las limitaciones técnicas o comerciales legítimas que impiden la conformidad con el requisito original. | |
| **2. Definición de los Controles Compensatorios** | Defina los controles compensatorios: explique cómo abordan los objetivos del control original y el aumento del riesgo si lo hay. | |
| **3. Objetivo** | Defina el objetivo del control original. | |
| | Identifique el objetivo que cumple el control compensatorio.<br>***Nota:** Este puede ser, pero no es obligatorio, el Objetivo del Enfoque Personalizado indicado para este requisito en PCI DSS.* | |
| **4. Riesgo Identificado** | Identifique cualquier riesgo adicional que suponga la falta del control original. | |
| **5. Validación de los Controles Compensatorios** | Defina cómo se validaron y comprobaron los controles compensatorios. | |
| **6. Mantenimiento** | Defina los procesos y controles establecidos para mantener los controles compensatorios. | |

## Anexo C: Explicación de los Requisitos Señalados como No Aplicable

*Se debe llenar un Anexo para cada requisito cuando se haya seleccionado No Aplicable.*

| Requisito | Razón por la cual el Requisito es No Aplicable |
|---|---|
| *Ejemplo:* | |
| *Requisito 3.5.1* | *Los datos del titular de la tarjeta nunca se almacenan electrónicamente* |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# Anexo D: Explicación de los Requisitos Señalados como No Probado

*Se debe llenar un Anexo para cada requisito cuando se haya seleccionado No Probado.*

| Requisito | Descripción del Requisito(s) No Probado | Describa por qué el Requisito(s) fue excluido de la Evaluación |
|---|---|---|
| *Ejemplos:* | | |
| *Requisito 10* | *No se probaron requisitos del Requisito 10.* | *Esta evaluación sólo cubre los requisitos del Hito1 del Enfoque Prioritario.* |
| *Requisitos 1-8, 10-12* | *Para esta evaluación sólo se revisó el Requisito 9. Todos los otros requisitos fueron excluidos.* | *El comerciante es un proveedor de alojamiento físico (CO-LO), y para esta evaluación sólo se han tenido en cuenta los controles de seguridad físicos.* |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Sección 3: Detalles de Validación y Certificación

## Parte 3. Validación PCI DSS

**Esta AOC se basa en los resultados anotados en el SAQ D (Sección 2), fechados (Fecha de finalización de la autoevaluación *DD-MM-AAAA* ).**

Indique a continuación si se ha realizado una evaluación PCI DSS completa o parcial:

☐ **Evaluación Completa -** Se han evaluado todos los requisitos, por lo tanto, no se ha marcado ningún requisito como No Probado en el SAQ.

☐ **Evaluación Parcial -** Uno o más requisitos no han sido evaluados y por lo tanto fueron marcados como No Probados en el SAQ. Cualquier requisito no evaluado se anota como No probado en la Parte 2g anterior.

Sobre la base de los resultados documentados en el SAQ D indicado anteriormente, cada firmante identificado en cualquiera de las Partes 3b-3d, según corresponda, afirma el siguiente estado de conformidad para el comerciante identificado en la Parte 2 de este documento.

***Seleccione uno:***

| | |
|---|---|
| ☐ | **En Conformidad:** Todas las secciones del PCI DSS SAQ están completas y todos los requisitos están marcados como 1) Implementado 2) Implementados con CCW, o 3) No Aplicable, lo que resulta en una calificación general de **EN CONFORMIDAD**; por lo tanto *(Nombre del Comerciante)* ha demostrado estar en conformidad con todos los Requisitos de PCI DSS incluidos en este SAQ con la excepción de aquellos marcados anteriormente como No Probados. |
| ☐ | **No Conformidad:** No se han completado todas las secciones del PCI DSS SAQ, o uno, o más requisitos están marcados como No Implementado, lo que resultada en una calificación general de **NO CONFORMIDAD**, por lo tanto *(Nombre del Comerciante)* no ha demostrado estar en conformidad con los Requisitos de PCI DSS incluidos en este SAQ.<br>**Fecha Límite** para estar en Conformidad: *DD-MM-AAAA*<br>El comerciante que envíe este formulario con un estado de No-Conformidad se le puede solicitar que complete el Plan de Acción en la Parte 4 de este documento. Confirme con la entidad a la que se presentará este AOC *antes de completar la Parte 4.* |
| ☐ | **Conforme pero con una excepción legal:** Uno o más de los requisitos evaluados en el PCI DSS SAQ están marcados como No Implementado debido a una restricción legal que impide que se cumpla con el requisito y todos los demás requisitos están marcados como 1) Implementado, 2) Implementado con CCW, o 3) No Aplicable, lo que da como resultado una calificación general de EN **CONFORMIDAD PERO CON EXCEPCIÓN LEGAL**; por lo tanto, *(Nombre del Comerciante)* ha demostrado estar en conformidad con todos los Requisitos de PCI DSS incluidos en este SAQ, excepto los señalados como No Implementados debido a una restricción legal.<br>Esta opción requiere una revisión adicional por parte de la entidad a la que se presentará este AOC.<br>*Si la selecciona, llene lo siguiente:* |

| Requisito Concerniente | Detalles de cómo la restricción legal impide que se cumpla con el requisito |
|---|---|
| | |
| | |
| | |

## Parte 3a. Reconocimiento del Comerciante

**El signatario confirma:**

***(Seleccione todo lo que aplican)***

| | |
|---|---|
| ☐ | El Cuestionario de Autoevaluación PCI DSS D, versión 4.0.1, ha sido completado de acuerdo con las instrucciones que en el figuran. |
| ☐ | Toda la información contenida en el cuestionario de autoevaluación SAQ y en esta declaración representan fielmente los resultados de la evaluación del comerciante en todos los aspectos materiales. |
| ☐ | Los controles PCI DSS se mantendrán en todo momento, según corresponda al entorno del comerciante. |

## Parte 3b. Declaración del Comerciante

| | |
|---|---|
| *Firma del Ejecutivo del Comerciante ↑* | *Fecha: DD-MM-AAAA* |
| *Nombre del Ejecutivo del Comerciante:* | *Título:* |

## Parte 3c. Declaración del Asesor de Seguridad Calificado (QSA)

| | |
|---|---|
| Si un QSA ha participado o asistido en esta evaluación, indique la función que desempeñó: | ☐ El QSA realizó los procedimientos de prueba. |
| | ☐ El QSA prestó otro tipo de asistencia.<br>Si ha seleccionado, describa todas las funciones desempeñadas: |

| | |
|---|---|
| *Firma del QSA principal ↑* | *Fecha: DD-MM-AAAA* |
| Nombre del QSA principal: | |

| | |
|---|---|
| *Firma del Funcionario Debidamente Autorizado de la Compañía QSA ↑* | *Fecha: DD-MM-AAAA* |
| *Nombre del Funcionario Debidamente Autorizado:* | *Compañía QSA:* |

## Parte 3d. Participación del Asesor de Seguridad Interna (ISA) del PCI SSC

| | |
|---|---|
| Si un ISA ha participado o ha prestado asistencia en esta Evaluación, indique la función desempeñada: | ☐ El ISA(s) realizó los procedimientos de prueba. |
| | ☐ El ISA(s) prestó otro tipo de asistencia.<br>Si ha seleccionado, describa todas las funciones desempeñadas: |

## Parte 4. Plan de Acción para Requisitos de No-Conformidad

*Sólo termine la Parte 4 si es solicitado por la entidad a la que se va a presentar este AOC, y sólo si la Evaluación presenta resultados de No-Conformidad señalados en la Sección 3.*

Si se le pide que rellene esta sección, seleccione la respuesta adecuada para "En Conformidad con los Requisitos de PCI DSS " para cada uno de los requisitos siguientes. Para cualquier respuesta "No", incluya la fecha en la que el comerciante espera poder cumplir en conformidad con el requisito y una breve descripción de las medidas que se están implementando para estar en conformidad.

| Requisito de PCI DSS | Descripción del Requisito | En Conformidad con los Requisitos de PCI DSS (Seleccione Uno) | | Rehabilitación Fecha y Acciones (Si selecciona "NO" para cualquier Requisito) |
|---|---|---|---|---|
| | | SÍ | NO | |
| 1 | Instalar y mantener los controles de seguridad de la red | ☐ | ☐ | |
| 2 | Aplicar configuraciones seguras a todos los componentes del sistema | ☐ | ☐ | |
| 3 | Proteger los datos del titular de la tarjeta almacenados | ☐ | ☐ | |
| 4 | Proteger los datos de tarjetahabiente con criptografía robusta durante la transmisión a través de redes abiertas y públicas | ☐ | ☐ | |
| 5 | Proteger todos los sistemas y redes de software malicioso | ☐ | ☐ | |
| 6 | Desarrollar y mantener sistemas y softwares seguros | ☐ | ☐ | |
| 7 | Restringir el acceso a los componentes del sistema y a los datos de tarjetahabiente según la necesidad de conocimiento de la empresa | ☐ | ☐ | |
| 8 | Identificar a los usuarios y autenticar el acceso a los componentes del sistema | ☐ | ☐ | |
| 9 | Restringir el acceso físico a los datos de tarjetahabiente | ☐ | ☐ | |
| 10 | Registrar y supervisar todos los accesos a los componentes del sistema y a los datos de tarjetahabiente | ☐ | ☐ | |
| 11 | Poner a prueba regularmente la seguridad de los sistemas y de las redes | ☐ | ☐ | |
| 12 | Respaldar la seguridad de la información con políticas y programas organizacionales | ☐ | ☐ | |
| Anexo A2 | Requisitos adicionales de PCI DSS para entidades que utilizan SSL/primeras versiones de TLS para conexiones de terminal POS POI presencial con tarjetas | ☐ | ☐ | |

***Nota:*** *El PCI Security Standards Council es un organismo de normas global que proporciona recursos para profesionales de la seguridad de los pagos que son desarrollados en colaboración con nuestra comunidad de partes interesadas. Nuestros materiales son aceptados en numerosos programas de cumplimiento en todo el mundo. Consulte con su organización de cumplimiento individual para asegurarse de que este formulario sea aceptado en su programa. Para obtener más información sobre PCI SSC y nuestra comunidad de partes interesadas, visite: https://www.pcisecuritystandards.org/about_us/.*