El Enfoque Prioritario para Lograr la Conformidad PCI DSS

El Estándar de Seguridad de Datos de Payment Card Industry (PCI DSS) proporciona una base de requisitos técnicos y operativos, organizados en 12 requisitos principales y requisitos de seguridad detallados. PCI DSS ha sido desarrollada para asegurar los datos de tarjetahabientes que son almacenados, procesados y/o transmitidos por comerciantes, proveedores de servicios y otras organizaciones (denominadas, colectivamente, "organizaciones" en lo sucesivo). Por su carácter integral, PCI DSS proporciona una gran cantidad de información sobre seguridad, tanta que algunos responsables de la seguridad de los datos de tarjetahabientes pueden preguntarse por dónde empezar. Con este fin, PCI Security Standards Council ofrece el Enfoque Prioritario para ayudar a las organizaciones a comprender cómo pueden reducir el riesgo en una fase más temprana de su recorrido por PCI DSS.

¿Qué es el Enfoque Prioritario?

El Enfoque Prioritario asigna todos los requisitos PCI DSS en seis hitos de seguridad basados en los riesgos destinados a ayudar a las organizaciones a protegerse de manera incremental contra los factores de mayor riesgo y las amenazas crecientes mientras se encuentran en el camino hacia la conformidad PCI DSS. Ningún hito único en el Enfoque Prioritario proporciona una seguridad integral, pero seguir sus directrices ayudará a las organizaciones a proteger los datos de tarjetahabientes con mayor rapidez. El Enfoque Prioritario y sus hitos (descritos en la página 2) están destinados a proporcionar los siguientes beneficios:

- Proporciona una hoja de ruta que una organización puede utilizar para abordar sus riesgos en orden de prioridad
- Permite obtener "victorias rápidas" utilizando un enfoque pragmático
- Apoya la planificación financiera y operativa
- Promueve indicadores de progreso objetivos y medibles
- Ayuda a promover la consistencia entre los evaluadores

ASPECTOS DESTACADOS

- Ayuda a las organizaciones a identificar los objetivos de mayor riesgo.
- Crea un lenguaje común en torno a los esfuerzos de implementación y evaluación de PCI DSS.
- Permite a las organizaciones demostrar el progreso de conformidad.

Objetivos del Enfoque Prioritario

El Enfoque Prioritario proporciona una hoja de ruta de los requisitos PCI DSS basados en el riesgo asociado con el almacenamiento, el procesamiento y/o la transmisión de datos de tarjetahabientes. La hoja de ruta ayuda a las organizaciones a priorizar los esfuerzos para lograr la conformidad, establecer hitos y reducir el riesgo de infracciones a los datos de tarjetahabientes en la fase más temprana del proceso de conformidad. Además, la hoja de ruta ayuda a los adquirentes a medir objetivamente las actividades de conformidad y la reducción de riesgos de las organizaciones. El Enfoque Prioritario se desarrolló después de revisar los datos de las infracciones reales y los comentarios de los Evaluadores de Seguridad Cualificados, los investigadores forenses y la Junta de Asesores de PCI Security Standards Council. La hoja de ruta no pretende ser un sustituto, un atajo o un enfoque provisional para la conformidad PCI DSS, ni es un marco único aplicable a todas las organizaciones.

Las preguntas sobre el uso del Enfoque Prioritario y cómo el uso del Enfoque Prioritario puede afectar a las obligaciones de conformidad de una organización deben dirigirse a su adquirente o a las marcas de pago ante las que una organización informa conformidad.

Hitos para Priorizar los Esfuerzos de Conformidad PCI DSS

El Enfoque Priorizado incluye seis hitos. La siguiente tabla resume los objetivos de alto nivel de cada hito.

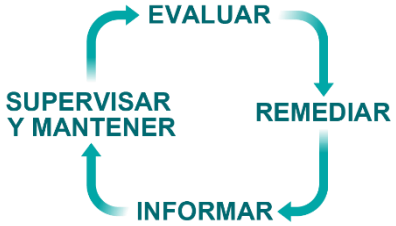
Hito	Objetivos
1	**No almacenar datos confidenciales de autenticación y limitar la retención de datos de tarjetahabientes.** Este hito se dirige a un área clave de riesgo para las entidades que se han visto comprometidas. Recuerde: si no se almacenan datos confidenciales de autenticación y otros datos de tarjetahabientes los efectos de un compromiso se reducirán en gran medida. Si no lo necesita, no lo almacene.
2	**Proteja los sistemas y las redes y esté preparado para responder a una infracción del sistema.** Este hito tiene como objetivo los controles de los puntos de acceso a la mayoría de los compromisos y a los procesos de respuesta.
3	**Aplicaciones de pago seguras.** Este hito se dirige a los controles de las aplicaciones, los procesos de aplicación y los servidores de aplicaciones. Los puntos débiles en estas áreas son presa fácil para comprometer los sistemas y obtener acceso a los datos de tarjetahabientes.
4	**Supervise y controle el acceso a sus sistemas.** Los controles de este hito le permiten detectar el quién, el qué, el cuándo y el cómo en relación con el acceso a su red y al entorno de datos de tarjetahabientes.
5	**Proteger los datos de tarjetahabientes almacenados.** Para aquellas organizaciones que han analizado sus procesos de negocio y han determinado que deben almacenar Números de Cuenta Primarios, este hito se centra en los mecanismos de protección clave para los datos almacenados.
6	**Finalice los esfuerzos de conformidad restantes y asegúrese de que todos los controles están implementados.** Este hito completa los requisitos PCI DSS y finaliza todas las políticas, procedimientos y procesos relacionados restantes necesarios para proteger el entorno de datos de tarjetahabientes.

Descargo de Responsabilidad

Este documento no modifica ni reduce a PCI DSS ni a ninguno de sus requisitos y puede ser modificado sin previo aviso.

PCI SSC no se hace responsable de los errores o daños de cualquier tipo resultantes del uso de la información aquí contenida. PCI SSC no ofrece ninguna garantía o representación en relación con la información proporcionada en este documento, y no asume ninguna responsabilidad en relación con el uso o el mal uso de dicha información.

LA CONFORMIDAD PCI DSS ES UN PROCESO CONTINUO



MARCAS DE PAGO PARTICIPANTES PCI SSC

Asignación de los Hitos del Enfoque Priorizado a los Requisitos de PCI DSS v4.0

El resto de este documento asigna los hitos a cada requisito y Sub-requisito PCI DSS v4.0. Tenga en cuenta que los requisitos PCI DSS v4.0 en la siguiente sección no incluyen las Notas de Aplicabilidad y otra información importante que se encuentra en PCI DSS. Las Notas de Aplicabilidad incluyen información que puede afectar a la interpretación de un requisito y se consideran una parte integral de PCI DSS que debe ser considerada en su totalidad durante una evaluación.

Las Notas de Aplicabilidad también indican los requisitos que son nuevos en PCI DSS v4.0 y que son las mejores prácticas hasta el 31 de marzo de 2025. Estos nuevos requisitos se indican con la siguiente nota: "Este Requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025; consulte las Notas de Aplicabilidad en PCI DSS para más detalles" en la tabla siguiente.

Se insta a las organizaciones a consultar a PCI DSS v4.0 para ver las Notas de Aplicabilidad y otra información importante incluida en ella.

ORGANIZACIONES PARTICIPANTES

Comerciantes, proveedores de servicios, bancos, procesadores, desarrolladores y vendedores de puntos de venta.

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
Requisito 1: Instalar y Mantener los Controles de Seguridad de la Red						
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 los procedimientos operativos que se identifican en el Requisito 1 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
1.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 1 están documentados, asignados y comprendidos.						6
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: • Definidos. • Implementados. • Mantenida.		2				
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.						6
1.2.3 Se mantienen los diagramas de red precisos que muestran todas las conexiones entre el CDE y otras redes, incluyendo las redes inalámbricas.	1					
1.2.4 Se mantienen diagramas de flujo de datos precisos que cumplen con lo siguiente: • Muestran todos los flujos de datos de tarjetahabientes a través de sistemas y redes. • Se actualizan según sea necesario ante cambios en el entorno.	1					
1.2.5 Todos los servicios, protocolos y puertos permitidos están identificados, aprobados y tienen una necesidad de negocio definida.		2				
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.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
1.2.7 Las configuraciones de los NSC se revisan al menos una vez cada seis meses para confirmar que son relevantes y eficientes.						6
1.2.8 Los archivos de configuración de los NSC están: • Asegurados contra el acceso no autorizado. • Se mantienen consistentes con las configuraciones de red activas.		2				
1.3 El acceso a la red hacia y desde el entorno de datos de tarjetahabientes está restringido.						
1.3.1 El tráfico de entrada al CDE está restringido de la siguiente manera: • Sólo al tráfico necesario. • Todo el resto del tráfico está específicamente denegado.		2				
1.3.2 El tráfico saliente del CDE se restringe de la siguiente manera: • Sólo al tráfico necesario. • Todo el resto del tráfico está específicamente denegado.		2				
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: • Todo el tráfico inalámbrico de las redes inalámbricas hacia el CDE es denegado de forma explícita. • Sólo se permite el tráfico inalámbrico al CDE que tenga un propósito de negocio autorizado.		2				
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 confiables y no confiables.		2				
1.4.2 El tráfico entrante de redes que no son confiables a redes confiables está restringido a: • Las comunicaciones con componentes del sistema autorizados para proveer servicios de acceso público, protocolos y puertos. • Respuestas las comunicaciones previamente iniciadas por componentes del sistema en una red confiable, esto para protocolos con dicho comportamiento. • Todo el tráfico restante está denegado.		2				
1.4.3 Se implementan medidas *Antispoofing* para detectar y bloquear la entrada a la red confiable de direcciones IP origen falsas o suplantadas.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
1.4.4 Los componentes del sistema que almacenan datos de tarjetahabientes no son accesibles directamente desde redes no confiables.		2				
1.4.5 La divulgación de las direcciones IP internas y la información de enrutamiento se limita sólo a las partes autorizadas.		2				
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: • Se definen los parámetros de configuración específicos para impedir que se introduzcan amenazas en la red de la entidad. • Los controles de seguridad se están ejecutando activamente. • 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.		2				
Requisito 2: Aplicar Configuraciones Seguras a Todos los Componentes del Sistema						
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 los procedimientos operativos que se identifican en el Requisito 2 están: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
2.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 2 son documentados, asignados y comprendidos.						6

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
2.2 Los componentes del sistema se configuran y administran de forma segura.						
2.2.1 Las estándares de configuración se desarrollan, implementan y mantienen para: • Cubrir todos los componentes del sistema. • Cubrir todas las vulnerabilidades de seguridad conocidas. • Brindar coherencia con los estándares de *hardening* del sistema aceptados por el sector o con las recomendaciones de *hardening* del proveedor. • Ser actualizadas a medida que se identifican nuevos problemas de vulnerabilidad, como se define en el Requisito 6.3.1. • 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.		2				
2.2.2 Las cuentas predeterminadas del proveedor se gestionan de la siguiente manera: • Si se utilizan las cuentas predeterminadas del proveedor, la contraseña predeterminada se cambia según el Requisito 8.3.6. • Si no se van a utilizar las cuentas predeterminadas del proveedor, la cuenta se elimina o se desactiva.		2				
2.2.3 Las funciones principales que requieren distintos niveles de seguridad se manejan como sigue: • Solo existe una función principal en un componente del sistema, **O** • Las funciones principales con distintos niveles de seguridad que existen en el mismo componente del sistema están aisladas entre sí, **O** • Las funciones primarias 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.		2				
2.2.4 Sólo se habilitan los servicios, protocolos, «demonios» y funciones necesarias, y se eliminan o deshabilitan todas las funciones innecesarias.		2				
2.2.5 Si existen servicios, protocolos o «demonios» inseguros: • La justificación de negocio está documentada. • Se documentan e implementan características de seguridad adicionales que reducen el riesgo de utilizar servicios, protocolos o «demonios» inseguros.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
2.2.6 Los parámetros de seguridad del sistema están configurados para impedir su uso indebido.		2				
2.2.7 Todo el acceso administrativo sin consola está cifrado utilizando criptografía robusta.		2				
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 de tarjetahabientes, todos los valores predeterminados de los proveedores inalámbricos se cambian en la instalación o se confirma que son seguros, incluidos, entre otros: • Claves de cifrado inalámbricas predeterminadas. • Contraseñas o puntos de acceso inalámbricos. • Valores predeterminados de SNMP. • Cualquier otro proveedor inalámbrico predeterminado relacionado con la seguridad.		2				
2.3.2 Para los entornos inalámbricos conectados al CDE o que transmitan datos de tarjetahabientes, las claves cifradas inalámbricas se cambian como sigue: • Siempre que el personal con conocimiento de la clave deje la empresa o la función para la que era necesario el conocimiento. • Siempre que se sospeche o se sepa que una clave está comprometida.		2				
Requisito 3: Proteger los Datos de Tarjetahabientes Almacenados						
3.1 Se definen y comprenden los procesos y mecanismos para proteger los datos almacenados de tarjetahabientes.						
3.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 3 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
3.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 3 están documentados, asignados y comprendidos.						6
3.2 El almacenamiento de los datos de tarjetahabientes se mantiene al mínimo.						

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
3.2.1 El almacenamiento de datos de tarjetahabientes se mantiene al mínimo mediante la implementación de políticas y procedimientos de retención y eliminación de datos que incluyan al menos lo siguiente: • Cubren todas las ubicaciones donde hay datos de tarjetahabientes. • Cubren todo dato confidencial de autenticación (SAD) almacenado antes de completar la autorización. *Este punto es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.* • Limitar la cantidad de datos almacenados y su tiempo de retención a lo requerido por los requisitos legales o reglamentarios y/o de negocios. • Requisitos de retención específicos para los datos de tarjetahabientes que definen la duración del período de retención e incluyen una justificación de negocio documentada. • Procesos para el borrado seguro o para hacer que los datos de tarjetahabiente sean irrecuperables cuando ya no se necesitan según la política de retención. • Un proceso para verificar, al menos una vez cada tres meses, que los datos de tarjetahabientes que excedan el período de retención definido se han eliminado de forma segura o se han vuelto irrecuperables.	1					
3.3 Los datos confidenciales de autenticación (SAD) no se almacenan después de la autorización.						
3.3.1 Los SAD no se retienen después de la autorización, incluso si están cifrados. Todos los datos confidenciales de autenticación recibidos se convierten en irrecuperables una vez finalizado el proceso de autorización.	1					
3.3.1.1 El contenido completo de cualquier pista no se conserva una vez finalizado el proceso de autorización.	1					
3.3.1.2 El código de verificación de la tarjeta no se conserva una vez finalizado el proceso de autorización.	1					
3.3.1.3 El número de identificación personal (PIN) y el bloque del PIN no se conservan al finalizar el proceso de autorización.	1					
3.3.2 Los SAD que se almacenan electrónicamente antes de completar la autorización se cifran mediante criptografía robusta. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*	1					

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
3.3.3 ***Requisito adicional para emisores y empresas que apoyan servicios de emisión y que almacenan datos confidenciales de autenticación:*** Cualquier almacenamiento de datos confidenciales de autenticación está: • Limitado a lo que se necesita para una necesidad legítima de negocio de emisión y está asegurado. • Cifrado utilizando criptografía robusta. *Este punto es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*	1					
3.4 El acceso a las pantallas de datos PAN completas y la capacidad de copiar los datos PAN está 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 negocio pueda ver **más que** el BIN y los últimos cuatro dígitos de los datos PAN.					5	
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*					5	
3.5 El número de cuenta principal (PAN) está protegido donde sea que se almacene.						
3.5.1 Los datos PAN se hace ilegible en cualquier lugar donde se almacene utilizando cualquiera de los siguientes enfoques: • *Hashes* unidireccionales basados en criptografía robusta del PAN completo. • Truncamiento (los *hashes* no pueden utilizarse para reemplazar el segmento truncado de la PAN). – 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. • Índice de *tokens.* • Criptografía robusta con procesos y procedimientos de gestión de claves asociados.					5	

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*					5	
3.5.1.2 Si se utiliza un cifrado 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: • En medios electrónicos extraíbles **O** • 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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*					5	
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: • El acceso lógico se gestiona por separado e independientemente de la autenticación del sistema operativo nativo y de los mecanismos de control de acceso. • Las claves de descifrado no están asociadas a las cuentas de usuarios. • 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.					5	

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
3.6 Las claves criptográficas utilizadas para proteger los datos almacenados de tarjetahabientes están protegidos.						
3.6.1 Los procedimientos se definen e implementan para proteger las claves cifradas utilizadas para proteger los datos almacenados de tarjetahabientes contra la divulgación y el uso indebido que incluyen: • El acceso a las claves está restringido al menor número de custodios necesarios. • Las claves de cifrado de claves son al menos tan seguras como las claves de cifrado de datos que estas protegen. • Las claves de cifrado de claves se almacenan por separado de las claves de cifrado de datos. • Las claves se almacenan de forma segura en el menor número posible de formas y ubicaciones.					5	
3.6.1.1 ***Requisito adicional sólo para proveedores de servicios:*** Se mantiene una descripción documentada de la arquitectura criptográfica que incluye: • Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos de tarjetahabientes, incluyendo la fuerza de la clave y la fecha de caducidad. • Evitar el uso de las mismas claves criptográficas en entornos de producción y de prueba. *Este punto es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.* • Descripción del uso de claves para cada clave. • Inventario de los módulos de seguridad de hardware (HSM), sistemas de gestión de claves (KMS) y otros dispositivos criptográficos seguros (SCD) utilizados para la gestión de claves, incluido el tipo y la ubicación de los dispositivos, como se describe en el Requisito 12.3.4.					5	
3.6.1.2 Las claves secretas y privadas que se utilizan para cifrar/descifrar los datos de tarjetahabientes se almacenan en uno (o más) de los siguientes formularios en todo momento: • 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. • 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. • Como mínimo dos componentes clave de longitud completa o recursos compartidos de clave, de acuerdo con un método aceptado por la industria.					5	

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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.					5	
3.6.1.4 Las claves criptográficas se almacenan en el menor número posible de ubicaciones.					5	
3.7 Cuando se usa criptografía para proteger datos almacenados de tarjetahabientes, 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 almacenados de tarjetahabientes.					5	
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 almacenados de tarjetahabientes.					5	
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 almacenados de tarjetahabientes.					5	
3.7.4 Se implementan políticas y procedimientos de gestión de claves para los cambios de claves criptográficas de para aquellas claves que han llegado al final de su criptoperíodo, según lo definido por el proveedor de la aplicación asociada o el propietario de la clave, y basado en las mejores prácticas y directrices de la industria, incluyendo lo siguiente: • Un criptoperíodo definido para cada tipo de clave en uso. • Un proceso para el cambio de claves al final del criptoperíodo definido.					5	
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 de tarjetahabientes, según se considere necesario cuando: • La clave haya llegado al final de su criptoperíodo definido. • 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. • Cuando se sospecha o se sabe que las claves están comprometidas. • Las claves retiradas o reemplazadas no se utilizan para operaciones de cifrado.					5	

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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.					5	
3.7.7 Se implementan políticas y procedimientos de administración de claves para incluir la prevención de la sustitución no autorizada de claves criptográficas.					5	
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.					5	
3.7.9 ***Requisito adicional sólo para proveedores de servicios:*** Cuando un proveedor de servicios comparte claves criptográficas con sus clientes para la transmisión o el almacenamiento de datos de tarjetahabiente, se documenta y distribuye a los clientes de los proveedores de servicios orientación sobre la transmisión, el almacenamiento y la actualización segura de dichas claves.					5	
Requisito 4: Proteger los Datos de Tarjetahabientes con una Criptografía Robusta Durante la Transmisión a Través de Redes Abiertas y Públicas						
4.1 Los procesos y mecanismos para proteger los datos de tarjetahabientes con criptografía robusta durante la transmisión a través de redes públicas abiertas están definidos y documentados.						
4.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 4 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
4.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 4 están documentados, asignados y comprendidos.						6

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
4.2 Los datos PAN está protegidos con criptografía robusta durante la transmisión.						
4.2.1 Se implementan fuertes protocolos de seguridad y criptografía robusta 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. • 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 la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.* • El protocolo en uso sólo apoya versiones o configuraciones seguras y no apoya el uso de versiones, algoritmos, tamaños de clave o implementaciones inseguras. • La fuerza del cifrado es apropiada para la metodología de cifrado en uso.		2				
4.2.1.1 Se mantiene un inventario de las claves y certificados confiables de la entidad utilizados para proteger los datos PAN durante la transmisión. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
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.		2				
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.		2				
Requisito 5: Proteger Todos los Sistemas y Redes de Software Malicioso						
5.1 Se definen y comprenden los procesos y mecanismos para proteger todos los sistemas y redes del software malicioso.						
5.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 5 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
5.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 5 están documentados, asignados y comprendidos.						6
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.*		2				
5.2.2 Las soluciones *antimalware* implementadas: • Detectan todos los tipos conocidos de *malware.* • Eliminan, bloquean o contienen todos los tipos conocidos de *malware.*		2				
5.2.3 Todos los componentes del sistema que no se encuentren en riesgo de *malware* se evalúan periódicamente para incluir lo siguiente: • Una lista documentada de todos los componentes del sistema que no están en riesgo de *malware*. • Identificación y evaluación de amenazas de *malware* en evolución para los componentes del sistema. • Confirmación de si dichos componentes del sistema continúan sin requerir protección *antimalware.*		2				
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
5.3 Los mecanismos y procesos *antimalware* están activos, mantenidos y monitoreados.						
5.3.1 Las soluciones *antimalware* se mantienen actualizadas a través de procesos de actualización automáticos.		2				
5.3.2 Soluciones antimalware: • Realizan escaneados periódicos y escaneados activos o en tiempo real. **O** • Realizan un análisis continuo del comportamiento de los sistemas o procesos.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
5.3.3 Para los medios electrónicos extraíbles, la solución *antimalware*: • Realiza escaneos automáticos cuando el medio es insertado, conectado o montado lógicamente, **O** • Realiza un análisis continuo del comportamiento de los sistemas o procesos cuando el medio está insertado, conectado o montado lógicamente. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
5.3.4 Los registros de auditoría de la solución *antimalware* están habilitados y se conservan de acuerdo con el Requisito 10.5.1.		2				
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.		2				
5.4 Los mecanismos contra *antiphishing* 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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
Requisito 6: Desarrollar y Mantener Sistemas y Softwares Seguros						
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: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
6.1.2 Las roles y responsabilidades para realizar las actividades del Requisito 6 están documentados, asignados y comprendidos.						6
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: • Basándose en estándares de la industria y/o mejores prácticas para un desarrollo seguro. • De acuerdo con PCI DSS (por ejemplo, autenticación segura y registro). • Considerando la incorporación de la información de problemas de seguridad durante cada etapa del ciclo de vida del desarrollo de software.			3			
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: • Sobre la seguridad del software relevante para su función laboral y lenguajes de desarrollo. • Incluyendo diseño de software seguro y técnicas de codificación segura. • Incluyendo, si se utilizan herramientas de prueba de seguridad, cómo utilizar las herramientas para detectar vulnerabilidades en el software.			3			
6.2.3 El software a 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: • Las revisiones de código garantizan que el código se desarrolle de acuerdo con las pautas de codificación segura. • Las revisiones de código buscan vulnerabilidades de software tanto existente como emergente. • Las correcciones apropiadas se implementan antes de la publicación.			3			

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • 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. • Revisados y aprobados por la dirección antes de su publicación.			3			
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 flujo de tipo comando, parámetro, objeto, defecto o de inyección. • 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). • 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.			3			

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • 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). • A las vulnerabilidades se les asigna una clasificación de riesgo basada en las mejores prácticas de la industria y considerando su impacto potencial. • Las clasificaciones de riesgo identifican, como mínimo, todas las vulnerabilidades consideradas de alto riesgo o críticas para el entorno. • Se cubren las vulnerabilidades de los programas informáticos a medida y de terceros (por ejemplo, sistemas operativos y bases de datos).			3			
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*			3			
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: • Los parches/actualizaciones críticas o de alta seguridad (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. • Todos los demás parches/actualizaciones de seguridad aplicables se instalan dentro de un período de tiempo apropiado según lo determine la entidad (por ejemplo, dentro de los tres meses posteriores al lanzamiento).			3			

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • 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: – Al menos una vez cada 12 meses y después de cambios significativos. – Por una entidad especializada en seguridad de aplicaciones. – Incluyendo, como mínimo, todos los ataques de software comunes descritos en el Requisito 6.2.4. – Todas las vulnerabilidades se clasifican de acuerdo con el Requisito 6.3.1. – Se corrigen todas las vulnerabilidades. – La aplicación se vuelve a evaluar después de las correcciones **O** • Instalación de soluciones técnicas automatizadas que detecten e impidan continuamente los ataques basados en la web de la siguiente manera: – Instaladas frente a las aplicaciones web de cara al público para detectar e impedir los ataques basados en la web. – Funcionando activamente y actualizándose según corresponda. – Generando registros de auditoría. – Configurados ya sea para bloquear los ataques basados en la web o para generar una alerta que se investigue inmediatamente.			3			
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: • Se instala frente a aplicaciones web de cara al público y está configurado para detectar e impedir ataques basados en la web. • Funcionando activamente y actualizándose según corresponda. • Generando registros de auditoría. • Configurados ya sea para bloquear los ataques basados en la web o para generar una alerta que se investigue inmediatamente. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*			3			

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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. • Se implementa un método para asegurar la integridad de cada *script*. • Se mantiene un inventario de todos los *scripts* con una justificación por escrito que explique su necesidad. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
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: • Motivo y descripción del cambio. • Documentación del impacto a la seguridad. • Aprobación documentada del cambio por las partes autorizadas. • Pruebas para verificar que el cambio no afecta negativamente la seguridad del sistema. • En el caso de los cambios de software a la medida y personalizados, todas las actualizaciones se comprueban para determinar la conformidad con el Requisito 6.2.4 antes de ser instalados para producción. • Procedimientos para hacer frente a los fallos y volver a un estado seguro.						6
6.5.2 Al completar un cambio significativo, se confirma que todos los requisitos PCI DSS están vigentes en todos los sistemas y redes nuevas o modificadas, y la documentación se actualiza según corresponda.						6
6.5.3 Los entornos de preproducción se separan de los entornos de producción y la separación se aplica con controles de acceso.			3			
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.			3			
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 PCI DSS aplicables.			3			

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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.			3			
Requisito 7: Restringir el Acceso a los Componentes del Sistema y a los Datos de Tarjetahabientes Según la Necesidad de Conocimiento de la Empresa						
7.1 Se definen y comprenden los procesos y mecanismos para restringir el acceso a los componentes del sistema ya los datos de tarjetahabientes según la necesidad de negocio.						
7.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 7 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
7.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 7 están documentados, asignados y son comprendidos.						6
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: • Acceso apropiado según el tipo de negocios de la entidad y las necesidades de acceso. • Acceso a los componentes del sistema y a los recursos de datos basados en la clasificación y las funciones del trabajo de los usuarios. • Los privilegios mínimos requeridos (por ejemplo, usuario, administrador) para realizar una función laboral.				4		
7.2.2 El acceso se asigna a los usuarios, incluidos los privilegiados, en función de: • La clasificación y función del trabajo. • Los privilegios mínimos necesarios para realizar las responsabilidades del trabajo.				4		
7.2.3 Los privilegios requeridos son aprobados por el personal autorizado.				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • Al menos una vez cada seis meses. • Para asegurarse de que las cuentas de usuario y el acceso sigan siendo apropiados según la función del trabajo. • Se aborda cualquier acceso inadecuado. • La gerencia reconoce que el acceso sigue siendo apropiado. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
7.2.5 Todas las aplicaciones y cuentas del sistema y los privilegios de acceso relacionados se asignan y administran de la siguiente manera: • Basado en los privilegios mínimos necesarios para la operatividad del sistema o aplicación. • El acceso está limitado a los sistemas, aplicaciones o procesos que específicamente requieren su uso. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
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: • 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). • El acceso a la aplicación/sistema sigue siendo apropiado para la función que se está realizando. • Se aborda cualquier acceso inadecuado. • La gerencia reconoce que el acceso sigue siendo apropiado. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
7.2.6 Todo acceso por parte de los usuarios a las bases de datos de tarjetahabientes está restringido de la siguiente manera: • A través de aplicaciones u otros métodos programáticos, con acceso y acciones permitidas basadas en las funciones y privilegios mínimos del usuario. • Solo los administradores autorizados pueden acceder directamente o consultar las bases de datos de CHD almacenados.				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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 Existen sistemas de control de acceso que restringen el acceso según la necesidad del usuario y cubre todos los componentes del sistema.				4		
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.				4		
7.3.3 El sistema de control de acceso está configurado para "denegar todo" predeterminadamente.				4		
Requisito 8: Identificar a los Usuarios y Autenticar el Acceso a los Componentes del Sistema						
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 son: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
8.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 8 están documentados, asignados y son comprendidos.						6
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 tarjetahabientes.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
8.2.2 Las cuentas grupales, 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: • Se impide el uso de la cuenta a menos que se requiera por una circunstancia excepcional. • Su uso está limitado al tiempo necesario para la circunstancia excepcional. • La justificación de negocio para su uso está documentada. • El uso está explícitamente aprobado por la dirección. • La identidad del usuario individual se confirma antes de que se conceda el acceso a una cuenta. • Cada acción realizada es atribuible a un usuario individual.		2				
8.2.3 ***Requisito adicional solo para proveedores de servicios:*** Los proveedores de servicios con acceso remoto a las instalaciones del cliente deben utilizar factores de autenticación únicos para las instalaciones de cada cliente.		2				
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: • Autorizado con la aprobación correspondiente. • Implementado solo con los privilegios especificados en la aprobación documentada.		2				
8.2.5 El acceso para los usuarios rescindidos se revoca inmediatamente.		2				
8.2.6 Las cuentas de usuario inactivas se eliminan o inhabilitan dentro de los 90 días de inactividad.		2				
8.2.7 Las cuentas utilizadas por terceros para acceder, dar apoyo o mantener componentes del sistema a través de acceso remoto se administran de la siguiente manera: • Son habilitadas solamente durante el período de tiempo necesario y son deshabilitadas cuando no están en uso. • El uso es monitoreado para detectar actividad inesperada.		2				
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.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • Algo que uno sabe, como una contraseña o frase de paso. • Algo que uno tiene, como un dispositivo *token* o una tarjeta inteligente. • Algo que uno es, como un elemento biométrico.		2				
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.		2				
8.3.3 La identidad del usuario se verifica antes de modificar cualquier factor de autenticación.		2				
8.3.4 Los intentos de autenticación inválidos se limitan mediante: • El bloqueo del *ID* de usuario después de no más de 10 intentos. • El establecimiento de la duración del bloqueo a un mínimo de 30 minutos o hasta que se confirme la identidad del usuario.		2				
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: • Se establece un valor único para la primera vez que se utilizan y al restablecerse. • Existe la obligatoriedad de cambiarlos inmediatamente después del primer uso.		2				
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: • Una longitud mínima de 12 caracteres (o SI el sistema no admite 12 caracteres, una longitud mínima de ocho caracteres). • Contener tanto caracteres numéricos como alfabéticos. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.* *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.*		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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.		2				
8.3.8 Las políticas y los procedimientos de autenticación están documentados y son comunicados a todos los usuarios, incluyendo: • Orientación sobre la selección de factores de autenticación robustos. • Orientación sobre cómo los usuarios deben proteger sus factores de autenticación. • Instrucciones para no reutilizar contraseñas/frases de paso utilizadas anteriormente. • 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.				4		
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: • Las contraseñas/frases de paso se cambian al menos una vez cada 90 días, **O** • 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.		2				
8.3.10 ***Requisito adicional solo para proveedores de servicios:*** Si las contraseñas / frases de paso contraseña se utilizan como el único factor de autenticación para el acceso del usuario del cliente a los datos de tarjetahabiente (es decir, en cualquier implementación de autenticación de factor único), entonces se brinda orientación a los usuarios del cliente, que incluye: • Orientación para que los clientes cambien sus contraseñas/frases de paso periódicamente. • Orientación sobre cuándo y bajo qué circunstancias se cambian las contraseñas/frases de paso.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
8.3.10.1 ***Requisito adicional sólo para proveedores de servicios:*** Si las contraseñas/frases de paso se utilizan como el único factor de autenticación para el acceso del usuario del cliente (es decir, en cualquier implementación de autenticación de factor único), entonces: • Las contraseñas/frases de paso se cambian al menos una vez cada 90 días, **O** • 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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
8.3.11 Cuando se utilizan factores de autenticación como *tokens* de seguridad físicos o lógicos, tarjetas inteligentes o certificados: • Los factores se asignan a un usuario individual y no se comparten entre varios usuarios. • Los controles físicos y/o lógicos garantizan que sólo el usuario previsto pueda utilizar ese factor para acceder.				4		
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.		2				
8.4.2 Los MFA se implementan para todos los ingresos al CDE. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
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 de la siguiente manera: • Todo acceso remoto por parte de todo el personal, tanto usuarios como administradores, originados fuera de la red de la entidad. • Todo acceso remoto por terceros y proveedores.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • El sistema MFA no es susceptible a ataques de repetición. • 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. • Se utilizan al menos dos tipos diferentes de factores de autenticación. • Se requiere el éxito de todos los factores de autenticación antes de que se otorgue el acceso. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
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: • Se impide el uso interactivo a menos que se requiera por una circunstancia excepcional. • El uso está limitado al tiempo necesario para la circunstancia excepcional. • La justificación de negocio para su uso interactivo está documentada. • El uso interactivo está explícitamente aprobado por la dirección. • La identidad del usuario individual se confirma antes de que se conceda el acceso a una cuenta. • Cada acción realizada es atribuible a un usuario individual. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • 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 con todos los elementos especificados en el Requisito 12.3.1) y ante la sospecha o la confirmación de que estén comprometidas. • 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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
Requisito 9: Restringir el Acceso Físico a los Datos de Tarjetahabientes						
9.1 Se definen y comprenden los procesos y mecanismos para restringir el acceso físico a los datos de tarjetahabientes.						
9.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 9 están: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
9.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 9 están documentados, asignados y comprendidos.						6
9.2 Los controles de acceso físico gestionan la entrada a las instalaciones y sistemas que contengan datos de tarjetahabientes.						
9.2.1 Existen controles de entrada a las instalaciones apropiados para restringir el acceso físico a los sistemas en el CDE.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
9.2.1.1 El ingreso 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: • Los puntos de entrada y salida hacia/desde las áreas sensibles dentro del CDE son monitorizados. • Los dispositivos o mecanismos de monitorización están protegidos contra la manipulación o la desactivación. • Los datos recogidos se revisan y se correlacionan con otras entradas. • Los datos recogidos se almacenan durante al menos tres meses, a menos que la ley lo restrinja.		2				
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.		2				
9.2.3 El ingreso 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.		2				
9.2.4 El acceso a las consolas en áreas sensibles está restringido mediante bloqueo cuando no están en uso.		2				
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: • Identificación de personal. • Gestionar cambios en los requisitos de ingreso físico de una persona. • Revocación o rescisión de la identificación del personal. • Limitar el acceso al proceso o sistema de identificación al personal autorizado.					5	
9.3.1.1 El acceso físico a áreas sensitivas dentro del CDE para el personal se controla de la siguiente manera: • El acceso está autorizado y se basa en la función del trabajo individual. • El acceso se revoca inmediatamente después de la terminación. • Todos los mecanismos de acceso físico, como llaves, tarjetas de acceso, etc., se devuelven o desactivan al finalizar.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
9.3.2 Se implementan procedimientos para autorizar y administrar el acceso de visitantes al CDE, que incluyen: • Los visitantes son autorizados antes de ingresar. • Los visitantes están acompañados en todo momento. • Los visitantes están claramente identificados y reciben un gafete u otra identificación con fecha de caducidad. • Los gafetes de visitante u otra identificación distinguen visiblemente a los visitantes del personal.					5	
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.					5	
9.3.4 Se utiliza un registro de visitantes para mantener un registro físico de las actividades de los visitantes dentro de la instalación y dentro de las áreas sensibles, que incluye: • El nombre del visitante y la organización representada. • La fecha y hora de la visita. • El nombre del personal que autoriza el acceso físico. • Conservar el registro al menos durante al menos tres meses, a menos que la ley lo restrinja.					5	
9.4 Los medios con datos de tarjetahabientes se almacenan, acceden, distribuyen y destruyen de forma segura.						
9.4.1 Todos los medios que contienen datos de tarjetahabientes están protegidos físicamente.					5	
9.4.1.1 Las copias de seguridad sin conexión con los datos de tarjetahabientes se almacenan en una ubicación segura.					5	
9.4.1.2 La protección de las ubicaciones de las copias de seguridad fuera de línea que contienen los datos de tarjetahabientes, se revisa al menos una vez cada 12 meses.					5	
9.4.2 Todos los datos de tarjetahabientes se clasifican de acuerdo con la confidencialidad de esos datos.					5	

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
9.4.3 Los apoyos con datos de tarjetahabientes enviados fuera de las instalaciones se protegen de la siguiente manera: • Los datos enviados fuera de las instalaciones se registran. • Los datos se envían por mensajería segura u otro método de entrega que pueda ser rastreado con precisión. • Los registros de seguimiento fuera de las instalaciones incluyen detalles sobre la ubicación de los datos.					5	
9.4.4 La gerencia aprueba todos los movimientos de apoyos con datos de tarjetahabientes que se trasladan fuera de las instalaciones (incluso cuando son distribuidos a particulares).					5	
9.4.5 Se mantienen registros de inventario de todos los apoyos electrónicos con datos de tarjetahabientes.					5	
9.4.5.1 Los inventarios de apoyos electrónicos con datos de tarjetahabientes se realizan al menos una vez cada 12 meses.					5	
9.4.6 Los materiales impresos con datos de tarjetahabientes se destruyen cuando ya no se necesitan por razones de negocios o legales, de la siguiente manera: • Los materiales se trituran transversalmente, se incineran o se pulverizan de forma que los datos de tarjetahabientes no puedan reconstruirse. • Los materiales se guardan en contenedores de almacenamiento seguro antes de su destrucción.	1					
9.4.7 Los medios de almacenamiento electrónicos con datos de tarjetahabientes se destruyen cuando ya no se necesitan por razones de negocio o legales mediante una de las siguientes opciones: • El medio de almacenamiento electrónico se destruye. • Los datos de tarjetahabientes se vuelven irrecuperables, de modo que no pueden reconstruirse.	1					

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
9.5 Los dispositivos de Punto de Interacción (POI) están protegidos contra manipulaciones y sustituciones no autorizadas.						
9.5.1 Los dispositivos POI que capturan los datos de las tarjetas de pago 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: • Mantener una lista de dispositivos de POI. • Inspeccionar periódicamente los dispositivos POI en busca de manipulaciones o sustituciones no autorizadas. • Formar al personal para que esté atento a los comportamientos sospechosos y denuncie las manipulaciones o sustituciones no autorizadas de los dispositivos.		2				
9.5.1.1 Se mantiene una lista actualizada de los dispositivos POI, que incluye: • Marca y modelo del dispositivo. • Ubicación del dispositivo. • Número de serie del dispositivo u otros métodos de identificación única.		2				
9.5.1.2 Las superficies de los dispositivos POI se inspeccionan periódicamente para detectar manipulaciones y sustituciones no autorizadas.		2				
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: manipulación o reemplazo de dispositivos POI, lo que incluye: • 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. • Procedimientos para garantizar que los dispositivos no se instalen, reemplacen o devuelvan sin verificación. • Ser consciente de comportamientos sospechosos alrededor de los dispositivos. • Informar sobre comportamientos sospechosos e indicaciones de manipulación o sustitución de dispositivos al personal apropiado.		2				
Requisito 10: Registrar y Supervisar Todos los Accesos a los Componentes del Sistema y a los Datos de Tarjetahabientes						
10.1 Se definen y documentan los procesos y mecanismos para ingresar y monitorear todos los accesos a los componentes del sistema y a los datos de tarjetahabientes.						
10.1.1 Todas las políticas de seguridad y procedimientos operativos que se identifican en el Requisito 10 está: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
10.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 10 están documentados, asignados y comprendidos.						6
10.2 Los registros de auditoría se implementan para apoyar la detección de anomalías y actividades sospechosas, y el análisis forense de eventos.				4		
10.2.1 Los registros de auditoría están habilitados y activos para todos los componentes del sistema y los datos de tarjetahabientes.				4		
10.2.1.1 Los registros de auditoría capturan todo el acceso de los usuarios individuales a los datos de tarjetahabientes.				4		
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.				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
10.2.1.3 Los registros de auditoría capturan todo el acceso a los mismos.				4		
10.2.1.4 Los registros de auditoría capturan todos los intentos de acceso lógico inválidos.				4		
10.2.1.5 Los registros de auditoría capturan todos los cambios en la identificación y credenciales de autenticación, lo que incluye, entre otros: • Creación de nuevas cuentas. • Elevación de privilegios. • Todos los cambios, adiciones o eliminaciones de cuentas con acceso administrativo.				4		
10.2.1.6 Los registros de auditoría capturan lo siguiente: • Toda inicialización de nuevos registros de auditoría y • Todo inicio, la detención o la pausa de los registros de auditoría existentes.				4		
10.2.1.7 Los registros de auditoría capturan toda la creación y eliminación de objetos a nivel del sistema.				4		
10.2.2 Los registros de auditoría guardan los siguientes detalles para cada evento auditable: • Identificación del usuario. • Tipo de evento. • Fecha y hora. • Indicación de Exitoso o Fallido. • Origen del evento. • Identidad o nombre de los datos, componentes del sistema, recursos o servicios afectados (por ejemplo, nombre y protocolo).				4		
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.				4		
10.3.2 Los archivos de registros de auditoría están protegidos para evitar modificaciones por parte de terceros.				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
10.3.3 Los archivos de registros de auditoría, incluidos los de tecnologías externas, se respaldan de inmediato en un servidor de registro interno seguro, central o sobre otro medio que sea difícil de modificar.				4		
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.				4		
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: • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD. • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, controles de seguridad de red, sistemas de detección de intrusiones/sistemas de prevención de intrusiones (IDS / IPS), servidores de autenticación).				4		
10.4.1.1 Se utilizan mecanismos automatizados para realizar revisiones de los registros de auditoría. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
10.4.2 Los registros de todos los demás componentes del sistema (aquellos no especificados en el Requisito 10.4.1) se revisan periódicamente.				4		
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
10.4.3 Se abordan las excepciones y anomalías identificadas durante el proceso de revisión.				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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 durante 12 meses como mínimo, teniendo al menos los tres últimos meses inmediatamente disponibles para su análisis.				4		
10.6 Los mecanismos de sincronización de la hora apoyan 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.				4		
10.6.2 Los sistemas están configurados con la hora correcta y consistente como sigue: • Uno o más servidores de tiempo designados están en uso. • Solo los servidores de hora central designados reciben la hora de fuentes externas. • La hora recibida de fuentes externas se basa en la Hora Atómica Internacional u Hora Universal Coordinada (UTC). • Los servidores de tiempo designados aceptan actualizaciones de tiempo solo de fuentes externas específicas aceptadas por la industria. • Cuando hay más de un servidor de tiempo designado, los servidores de tiempo se emparejan entre sí para mantener la hora exacta. • Los sistemas internos reciben información de la hora solo de los servidores de hora central designados.				4		
10.6.3 La configuración de sincronización de la hora y los datos están protegidos de la siguiente manera: • El acceso a los datos de tiempo está restringido solo al personal con una necesidad de negocio. • Cualquier cambio en la configuración de tiempo en sistemas críticos se registra, monitorea y verifica.				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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:*** Las fallas de los sistemas de control de seguridad críticos se detectan, alertan y abordan de inmediato, incluyendo entre otras, las fallas de los siguientes sistemas de control de seguridad críticos: • Controles de seguridad de la red. • IDS/IPS. • FIM. • Soluciones antimalware. • Controles de acceso físico. • Controles de Ingreso lógico. • Mecanismos de registro de auditoría. • Controles de segmentación (si se utilizan).				4		
10.7.2 Las fallas de los sistemas de control de seguridad críticos se detectan, alertan y abordan de inmediato, incluidas, entre otras, las fallas de los siguientes sistemas de control de seguridad críticos: • Controles de seguridad de la red. • IDS/IPS. • Cambiar los mecanismos de detección. • Soluciones antimalware. • Controles de acceso físico. • Controles de Ingreso lógico. • Mecanismos de registro de auditoría. • Controles de segmentación (si se utilizan). • Mecanismos de revisión del registro de auditoría. • Herramientas de prueba de seguridad automatizadas (si se utilizan). *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
10.7.3 Las fallas de cualquier sistema de control de seguridad crítico se responden con prontitud, incluidas, entre otras, las siguientes: • Restaurando las funciones de seguridad. • Identificando y documentando la duración (fecha y hora de principio a fin) de la falla de seguridad. • Identificando y documentando las causas de la falla y documentando el remedio requerido. • Identificando y abordando cualquier problema de seguridad que surgió durante la falla. • Determinar si se requieren más acciones como resultado de la falla de seguridad. • Implementar controles para evitar que se repita la causa de la falla. • Reanudación del monitoreo de los controles de seguridad. *Este es un requisito PCI DSS v3.2.1que aplica solo a los proveedores de servicios. Este Requisito es la mejor práctica para todas las demás entidades hasta el 31 de marzo de 2025; consulte las Notas de Aplicabilidad en PCI DSS para más detalles.*				4		
Requisito 11: Poner a Prueba Regularmente la Seguridad de los Sistemas y de las Redes						
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: • Documentados. • Actualizados. • En uso. • Conocidos por todas las partes involucradas.						6
11.1.2 Los roles y responsabilidades para realizar las actividades del Requisito 11 son documentados, asignados y comprendidos.						6
11.2 Se identifican y controlan los puntos de acceso inalámbricos y se abordan los puntos de acceso inalámbricos no autorizados.						

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
11.2.1 Los puntos de acceso inalámbricos autorizados y no autorizados se gestionan de la siguiente manera: • Se comprueba la existencia de puntos de acceso inalámbricos *(Wi-Fi)* para, • Detectar e identificar todos los puntos de acceso inalámbricos autorizados y no autorizados, • Que la verificación, detección e identificación ocurre al menos cada tres meses. • Si se utiliza la supervisión automatizada, se notifica al personal mediante la generación de alertas.				4		
11.2.2 Se mantiene un inventario de los puntos de acceso inalámbricos autorizados, incluyendo una justificación de negocio documentada.				4		
11.3 Las vulnerabilidades externas e internas se identifican, se priorizan y se abordan periódicamente.						
11.3.1 Los escaneos de vulnerabilidad interna se realizan de la siguiente manera: • Al menos una vez cada tres meses. • Se resuelven las vulnerabilidades críticas y de alto riesgo (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1). • Se realizan re-escaneos que confirman que se han resuelto todas las vulnerabilidades críticas y de alto riesgo (como se indicó anteriormente). • La herramienta de escaneo se mantiene actualizada con la información más reciente sobre vulnerabilidades. • Los escaneos son realizados por personal calificado con la independencia organizacional del probador.		2				
11.3.1.1 Todas las demás vulnerabilidades aplicables (aquellas que no se clasifican como de alto riesgo o críticas (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1) se gestionan de la siguiente manera: • 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. • Los re-escaneos se realizan según sea necesario. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
11.3.1.2 Los escaneos de vulnerabilidad interna se realizan mediante escaneos autenticados como sigue: • Los sistemas que no pueden aceptar credenciales para los escaneos autentificados están documentados. • 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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
11.3.1.3 Los escaneos de vulnerabilidad interna se realizan después de cualquier cambio significativo como sigue: • Se resuelven las vulnerabilidades críticas y de alto riesgo (según las clasificaciones de riesgo de vulnerabilidad de la entidad definidas en el Requisito 6.3.1). • Los re-escaneos se realizan según sea necesario. • Los escaneos son realizados por personal cualificado con la independencia organizacional del probador (no se requiere que sea un QSA o ASV).		2				
11.3.2 Los escaneos de vulnerabilidad externa se realizan de la siguiente manera: • Al menos una vez cada tres meses. • Por parte de un Proveedor de Escaneo Aprobado por PCI SSC (ASV). • Las vulnerabilidades se resuelven y se cumple con los requisitos de la *Guía del Programa ASV.* • 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* de escaneos aprobados.		2				
11.3.2.1 Los escaneos de vulnerabilidad externa se realizan después de cualquier cambio significativo de la siguiente manera: • Se resuelven las vulnerabilidades calificadas con 4.0 o más por CVSS. • Los re-escaneos se realizan según sea necesario. • Los escaneos son realizados por personal cualificado con la independencia organizacional del probador (no se requiere que sea un QSA o ASV).		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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: • Enfoques de pruebas de penetración aceptados por la industria. • Cobertura para todo el perímetro de CDE y sus sistemas críticos. • Pruebas tanto dentro como fuera de la red. • Pruebas para validar cualquier control de segmentación y reducción del alcance. • Pruebas de penetración a nivel de la aplicación para identificar, como mínimo, las vulnerabilidades enumeradas en el Requisito 6.2.4. • Las pruebas de penetración a nivel de red que abarcan todos los componentes que apoyan las funciones de red y los sistemas operativos. • Revisión y consideración de amenazas y vulnerabilidades experimentadas en los últimos 12 meses. • Enfoque documentado para evaluar y abordar el riesgo que plantean las vulnerabilidades explotables y las debilidades de seguridad encontradas durante las pruebas de penetración. • Retención de los resultados de las pruebas de penetración y los resultados de las actividades de remediación durante al menos 12 meses.		2				
11.4.2 Se realizan pruebas de penetración interna: • Según la metodología definida por la entidad. • Al menos una vez cada 12 meses. • Después de cualquier actualización o cambio significativo de infraestructura o aplicación. • Por un recurso interno calificado o un tercero externo calificado. • El evaluador cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).		2				
11.4.3 Se realizan pruebas de penetración externa: • Según la metodología definida por la entidad. • Al menos una vez cada 12 meses. • Después de cualquier actualización o cambio significativo de infraestructura o aplicación. • Por un recurso interno calificado o un tercero externo calificado. • El evaluador cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
11.4.4 Las vulnerabilidades explotables y las debilidades de seguridad encontradas durante las pruebas de penetración se corrigen de la siguiente manera: • 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. • La prueba de penetración se repite para verificar las correcciones.		2				
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: • Al menos una vez cada 12 meses y después de cualquier cambio en los controles/métodos de segmentación. • Cubriendo todos los controles/métodos de segmentación en uso. • De acuerdo con la metodología de prueba de penetración definida por la entidad. • Confirmar que los controles/métodos de segmentación son operativos y eficientes, y aislar al CDE de todos los sistemas fuera del ámbito. • Confirmar la efectividad de cualquier uso de aislamiento para separar sistemas con diferentes niveles de seguridad (ver Requisito 2.2.3). • Realizado por un recurso interno calificado o un tercero externo calificado. • El evaluador cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).		2				
11.4.6 ***Requisito adicional sólo para proveedores de servicios:*** 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: • Al menos una vez cada seis meses y después de cualquier cambio en los controles/métodos de segmentación. • Cubriendo todos los controles/métodos de segmentación en uso. • De acuerdo con la metodología de prueba de penetración definida por la entidad. • Confirmar que los controles/métodos de segmentación son operativos y eficientes, y aislar al CDE de todos los sistemas fuera del ámbito. • Confirmar la efectividad de cualquier uso de aislamiento para separar sistemas con diferentes niveles de seguridad (ver Requisito 2.2.3). • Realizado por un recurso interno calificado o un tercero externo calificado. • El evaluador cuenta con independencia organizacional (no se requiere que sea un QSA o ASV).		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
11.4.7 ***Requisito adicional sólo para proveedores de servicios multiusuario:*** Los proveedores de servicios multiusuario apoyan a sus clientes para las pruebas de penetración externas según los Requisitos 11.4.3 y 11.4.4. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
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: • Todo el tráfico se supervisa en el perímetro del CDE. • Todo el tráfico se supervisa en los puntos críticos del CDE. • Se envía una alerta al personal indicando las sospechas de situaciones comprometidas. • Todos los motores de detección y prevención de intrusiones, las líneas de base y las firmas se mantienen actualizadas.		2				
11.5.1.1 ***Requisito adicional sólo para proveedores de servicios:*** Las técnicas de detección-intrusión y/o intrusión-prevención detectan, alertan/impiden y abordan los canales de comunicación de malware encubierto. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
11.5.2 Un mecanismo de detección de cambios (por ejemplo, herramientas de monitoreo de integridad de archivos) se despliega como sigue: • Para alertar al personal sobre modificaciones no autorizadas (incluyendo cambios, adiciones y eliminaciones) de archivos críticos. • Para realizar comparaciones de archivos críticos al menos una vez por semana.				4		
11.6 Se detectan los cambios no autorizados en las páginas de pago se detectan y se responden.						

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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 y en el contenido de las páginas de pago tal y como las recibe el navegador del consumidor. • El mecanismo está configurado para evaluar el encabezamiento HTTP y la página de pago recibidas. • Las funciones del mecanismo se realizan de la siguiente manera: – Al menos una vez cada siete días **O** – 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). *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
Requisito 12: Respaldar la Seguridad de la Informácion con Políticas y Programas Organizacionales						
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 informática es: • Establecida. • Publicada. • Mantenida. • Difundida a todo el personal relevante, así como a los proveedores y socios comerciales relevantes.						6
12.1.2 La política de seguridad de la información es: • Revisada al menos una vez cada 12 meses. • Actualizada según sea necesario para reflejar los cambios en los objetivos de negocios o en los riesgos para el entorno.						6
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.						6

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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.						6
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: • Aprobación explícita por las partes autorizadas. • Usos aceptables de la tecnología. • Lista de productos aprobados por el comerciante para uso de los empleados, incluidos hardware y software.						6
12.3 Los riesgos para el entorno de datos de tarjetahabientes se identifican, evalúan y gestionan formalmente.						
12.3.1 Cada requisito PCI DSS que proporciona flexibilidad sobre la frecuencia con la que se realizan (por ejemplo, los requisitos que deben realizarse periódicamente) están apoyados por un análisis de riesgo específico que está documentado e incluye: • Identificación de los activos a proteger. • Identificación de las amenazas contra las que protege el requisito. • Identificación de factores que contribuyen a la probabilidad y/o impacto de que se materialice una amenaza. • Análisis resultante que determine e incluya la justificación de la frecuencia con la que se debe realizar el requisito para minimizar la probabilidad de que se materialice la amenaza. • 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. • Realización de análisis de riesgos actualizados cuando sea necesario, según lo determinado por la revisión anual. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
12.3.2 Se realiza un análisis de riesgos específico para cada Requisito PCI DSS que la entidad reúne con el enfoque personalizado, que incluye: • Evidencia documentada que detalla cada elemento se especifica en el Anexo D: Enfoque Personalizado (incluyendo, como mínimo, una matriz de controles y un análisis de riesgos). • Aprobación de las evidencias documentadas por parte de la alta dirección. • La realización del análisis de riesgos específico al menos una vez cada 12 meses.		2				
12.3.3 Los conjuntos de cifrado criptográfico y los protocolos en uso se documentan y revisan al menos una vez cada 12 meses, incluyendo al menos lo siguiente: • Un inventario actualizado de todos los protocolos y conjuntos de cifrado criptográfico en uso, incluyendo su propósito y dónde se utilizan. • 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. • Una estrategia documentada para responder a los cambios anticipados en las vulnerabilidades criptográficas. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*						6
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: • Análisis de que las tecnologías continúan recibiendo correcciones de seguridad por parte de los proveedores con prontitud. • Análisis de que las tecnologías continúan apoyando (y no imposibilitan) la conformidad PCI DSS de la entidad. • 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. • 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". *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*						6

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
12.4 Gestión del cumplimiento con PCI DSS.						
12.4.1 ***Requisito adicional solo para proveedores de servicios:*** La responsabilidad es establecida por la gerencia ejecutiva para la protección de datos de tarjetahabientes y un programa de conformidad PCI DSS que incluye: • Responsabilidad general para mantener la conformidad PCI DSS. • Definición de un estatuto para un programa de conformidad PCI DSS y un reporte a la dirección ejecutiva.						6
12.4.2 ***Requisito adicional solo para proveedores de servicios:*** Las revisiones se realizan al menos una vez cada tres meses para confirmar que el personal está realizando sus tareas de acuerdo con todas las políticas de seguridad y los procedimientos operativos. Las revisiones son realizadas por personal distinto al responsable de realizar la tarea en cuestión e incluyen, entre otras, las siguientes tareas: • Revisiones de registros diarios. • Revisiones de configuración para controles de seguridad de la red. • Aplicación de estándares de configuración a nuevos sistemas. • Respuesta a las alertas de seguridad. • Procesos de gestión del cambio.						6
12.4.2.1 ***Requisito adicional solo para proveedores de servicios:*** Las revisiones realizadas de acuerdo con el Requisito 12.4.2 se documentan para incluir: • Resultados de las revisiones. • Acciones de remediación documentadas tomadas para cualquier tarea que no se haya realizado en el Requisito 12.4.2. • Revisión y aprobación de los resultados por parte del personal al que se le haya asignado la responsabilidad del programa de conformidad PCI DSS.						6
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.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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. 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). • 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 de tarjetahabientes, 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. • 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 de tarjetahabientes, componentes del sistema, controles de segmentación y conexiones de terceros con acceso al CDE están incluidos en el alcance.	1					
12.5.2.1 ***Requisito adicional solo para proveedores de servicios:*** El alcance PCI DSS es documentado y confirmado por la entidad al menos una vez cada seis meses y ante cambios significativos en el entorno dentro del alcance. Como mínimo, la validación del alcance incluye todos los elementos especificados en el Requisito 12.5.2. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*	1					
12.5.3 ***Requisito adicional solo para proveedores de servicios:*** Los cambios significativos en la estructura organizativa dan como resultado una revisión documentada (interna) del impacto en el alcance PCI DSS y la aplicabilidad de los controles; los resultados se comunican a la dirección ejecutiva. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*						6

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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 tarjetahabientes.						6
12.6.2 El programa de concientización sobre seguridad es: • Revisado al menos una vez cada 12 meses, y • Actualizado según sea necesario para abordar cualquier nueva amenaza y vulnerabilidad que pueda impactar la seguridad del CDE de la entidad, o la información proporcionada al personal sobre sus funciones en lo concerniente a la protección de los datos de tarjetahabientes. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*						6
12.6.3 El personal recibe capacitación sobre seguridad de la siguiente manera: • Al momento de la contratación y al menos una vez cada 12 meses. • Se utilizan múltiples métodos de comunicación. • 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.						6
12.6.3.1 El entrenamiento de concientización de seguridad incluye la concientización ante amenazas y vulnerabilidades que podrían impactar la seguridad del CDE, incluyendo, pero no limitado a: • *Phishing* y ataques relacionados. • Ingeniería social. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*						6
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*						6

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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.						6
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 de tarjetahabientes o que podrían afectar a la seguridad de los datos de tarjetahabientes, incluyendo una descripción para cada uno de los servicios prestados.		2				
12.8.2 Se mantienen acuerdos escritos con los TPSP de la siguiente manera: • Se mantienen acuerdos escritos con todos los TPSP con los que se comparten datos de tarjetahabientes o que podrían afectar la seguridad del CDE. • Los acuerdos escritos incluyen el reconocimiento por parte de los TPSP de que son responsables por la seguridad de los datos de tarjetahabientes 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 del CDE de la entidad.		2				
12.8.3 Se implementa un proceso establecido para contratar a los TPSP, incluyendo la debida diligencia antes de la contratación.		2				
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.		2				
12.8.5 Se mantiene información sobre qué requisitos PCI DSS gestiona cada TPSP, cuáles gestiona la entidad y cualquiera que se comparta entre el TPSP y la entidad.		2				
12.9 Los proveedores de servicios externos (TPSP) apoyan la conformidad PCI DSS de sus clientes.						
12.9.1 ***Requisito adicional solo para proveedores de servicios:*** Los TPSP reconocen por escrito a los clientes que son responsables por la seguridad de los datos de tarjetahabientes que el TPSP posee o almacena, procesa o transmite en nombre del cliente, o en la medida en que puedan afectar la seguridad del CDE del cliente.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
12.9.2 ***Requisito adicional solo para proveedores de servicios:*** Los TPSP apoyan las solicitudes de información de sus clientes para cumplir con los Requisitos 12.8.4 y 12.8.5 proporcionando lo siguiente a pedido del cliente: • Información del estado de conformidad PCI DSS para cualquier servicio que el TPSP realice en nombre de los clientes (Requisito 12.8.4). • Información sobre qué requisitos PCI DSS son responsabilidad del TPSP y cuáles son responsabilidad del cliente, incluyendo las responsabilidades compartidas (Requisito 12.8.5).		2				
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: • 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. • Procedimientos de respuesta a incidentes con actividades específicas de contención y mitigación para diferentes tipos de incidentes. • Procedimientos de recuperación y continuidad del negocio. • Procesos de apoyo de datos. • Análisis de requisitos legales para reportar situaciones comprometidas. • Cobertura y respuestas de todos los componentes críticos del sistema. • Referencia o inclusión de procedimientos de respuesta a incidentes de las marcas de pago.		2				
12.10.2 Al menos una vez cada 12 meses, el plan de respuesta a incidentes de seguridad es: • Revisado y el contenido se actualiza según sea necesario. • Probado, incluyendo todos los elementos enumerados en el Requisito 12.10.1.		2				
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.		2				
12.10.4 El personal responsable de responder a incidentes de seguridad sospechados y confirmados recibe capacitación adecuada y periódica sobre sus responsabilidades en cuanto a la respuesta a incidentes.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
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. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
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: • Sistemas de detección y prevención de intrusiones. • Controles de seguridad de la red. • Mecanismos de detección de cambios en archivos críticos. • El mecanismo de detección de cambios y manipulaciones en las páginas de pago. *Este punto es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.* • Detección de puntos de acceso inalámbricos no autorizados.		2				
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.		2				
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: • 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. • Identificar si los datos confidenciales de autenticación se almacenan con datos de PAN. • Determinar de dónde proceden los datos de tarjetahabientes y cómo han llegaron donde no se esperaba. • Remediar fugas de datos o brechas en el proceso que llevaron a que los datos del tarjetahabientes llegaran a una ubicación inesperada. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
Anexo A1: Requisitos Adicionales de PCI DSS para Proveedores de Servicios Multiusuario						
A1.1 Los proveedores de servicios multiusuario protegen y separan todos los entornos y datos de los clientes.						
A1.1.1 La separación lógica se implementa de la siguiente manera: • El proveedor no puede ingresar a los entornos de sus clientes sin autorización. • Los clientes no pueden ingresar al entorno del proveedor sin autorización. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*				4		
A1.1.2 Los controles se implementan de modo que cada cliente solo tenga permiso para ingresar a sus propios datos de tarjetahabientes y CDE.				4		
A1.1.3 Los controles se implementan de modo que cada cliente solo pueda ingresar a los recursos que se le han asignados.				4		
A1.1.4 La eficiencia de los controles de separación lógica utilizados para separar los entornos de los clientes se confirma al menos una vez cada seis meses mediante pruebas de penetración. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
A1.2 Los proveedores de servicios multiusuario facilitan el registro y la respuesta a incidentes para todos los clientes.						
A1.2.1 La función de registro de auditoría está habilitada para el entorno de cada cliente de conformidad con el Requisito 10 PCI DSS, que incluye lo siguiente: • Los registros están habilitados para aplicaciones comunes de terceros. • Los registros están activos de forma predeterminada. • Los registros están disponibles para revisión solo por parte del cliente propietario. • Las ubicaciones de los registros se comunican claramente al cliente propietario. • Los datos de registro y la disponibilidad son consistentes con el Requisito 10 de los PCI DSS.				4		

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
A1.2.2 Se implementan procesos o mecanismos para apoyar y/o facilitar investigaciones forenses rápidas en caso de un incidente de seguridad sospechado o confirmado para cualquier cliente.		2				
A1.2.3 Se implementan procesos o mecanismos para reportar y abordar vulnerabilidades e incidentes de seguridad presuntos o confirmados, incluyendo lo siguiente: • Los clientes pueden informar de forma segura los incidentes de seguridad y las vulnerabilidades al proveedor. • El proveedor aborda y repara los incidentes de seguridad y las vulnerabilidades sospechadas o confirmadas de acuerdo con el Requisito 6.3.1. *Este requisito es la mejor práctica recomendada hasta el 31 de marzo de 2025, consulte las Notas de Aplicabilidad de PCI DSS para obtener más detalles.*		2				
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						
A2.1 Está confirmado que Los terminales POI que utilizan SSL y/o versiones iniciales de TLS no son susceptibles a explotaciones conocidas de SSL/TLS.						
A2.1.1 Cuando los terminales POS POI en el comercio 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.		2				
A2.1.2 ***Requisito adicional sólo para proveedores de servicios:*** Todos los proveedores de servicios con puntos de conexión existentes POS POI que utilizan SSL y/o primeras versiones de TLS como se define en A2.1 cuentan con un Plan de Migración y Mitigación de Riesgos que incluye: • Descripción del uso, incluidos los datos que se transmiten, los tipos y la cantidad de sistemas que usan y/o apoyan SSL/primeras versiones de TLS y el tipo de entorno. • Resultados de la evaluación de riesgos y controles de reducción de riesgos implementados. • Descripción de procesos para monitorear nuevas vulnerabilidades relacionadas con SSL/primeras versiones de TLS. • Descripción de los procesos de control de cambios que se implementan para garantizar que los SSL/primeras versiones de TLS no se implementen en nuevos entornos. • Descripción general del plan del proyecto de migración para reemplazar los SSL/primeras versiones de TLS en una fecha futura.		2				

Requisitos de PCI DSS v4.0	Hito					
	1	2	3	4	5	6
A2.1.3 ***Requisito Solo Para Proveedores de Servicios:*** Todos los proveedores de servicios brindan una oferta de servicios segura.		2				

DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerar se, 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.