Payment Card Industry

Estándar de Seguridad de Datos

Resumen de Cambios de la Versión PCI DSS 3.2.1 a la 4.0

Revisión 2

Diciembre de 2022

Cambios en los Documentos

Fecha	Revisión	Descripción
Marzo de 2022		Divulgación inicial del Resumen de Cambios en PCI DSS v3.2.1 a v4.0.
Mayo de 2022	1	Actualización de errata para corregir la descripción de cambios en el Requisito 8.3.9 de PCI DSS v4.0.
Diciembre de 2022	2	Actualización de errata para añadir la descripción del cambio realizado en el Requisito 6.3.3 y para corregir la entrada del la Tabla Resumen de Nuevos Requisitos para el Requisito 3.6.1.1.

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

Tabla de Contenido

1 Introducción

Este documento proporciona un resumen de alto nivel al describir los cambios de PCI DSS v3.2.1 a PCI DSS v4.0 y no detalla todas las revisiones del documento. Debido a la magnitud de los cambios, el estándar debe revisarse en su totalidad en lugar de centrarse únicamente en este documento resumido.

Este Resumen de los Cambios está organizado de la siguiente manera:

- *Tipos de Cambios* - proporciona una visión general de los tipos de cambios.
- *Resumen de los Cambios para las Secciones Introductorias de PCI DSS* - resume los cambios realizados para todas las secciones afectadas.
- *Resumen de los Cambios Generales en los Requisitos de PCI DSS* - resume los cambios realizados en todos los requisitos, procedimientos de prueba y orientaciones.
- *Cambios Adicionales por Requisito* - resume los cambios adicionales realizados en los requisitos 1-12 y en sus anexos.
- *Resumen de los Nuevos Requisitos* - enumera todos los nuevos requisitos, la entidad a la cual aplica el nuevo requisito (es decir, todas las entidades o sólo los proveedores de servicios) y la fecha de entrada en vigor del nuevo requisito.

2 Tipos de Cambios

Tipo de Cambio	Definición
Requisito en Evolución	Cambios para garantizar que el estándar esté al día ante las amenazas y tecnologías emergentes, y con los cambios en la industria de pagos. Los ejemplos incluyen requisitos o procedimientos de prueba nuevos o modificados, o la eliminación de un requisito.
Aclaración u Orientación	Actualizaciones en la redacción, explicaciones, definiciones, orientaciones adicionales y/o instrucciones para aumentar la comprensión o proporcionar mayor información u orientación sobre un tema en particular.
Estructura o formato	Reorganización del contenido, incluyendo la combinación, separación y el volver a enumerar los requisitos para alinear el contenido.

3 Resumen de los Cambios en las Secciones Introductorias de PCI DSS

Sección		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Introducción y Generalidades del Estándar de Seguridad de los datos PCI	Introducción y Generalidades del Estándar de Seguridad de datos PCI	Se ha añadido el subtítulo "Limitaciones" y se ha aclarado que PCI DSS no sustituye a las leyes locales, estatales o del condado. Se ha ampliado la lista de recursos de PCI DSS.	Aclaración u Orientación
Información sobre la Aplicabilidad de PCI DSS	Información sobre la Aplicabilidad de PCI DSS	Se han añadido sub-rúbricas para aumentar la legibilidad. Se ha aclarado que algunos requisitos de PCI DSS pueden aplicarse a las entidades que no almacenan, procesan o transmiten el número de cuenta principal (datos PAN). Se ha aclarado que los términos datos de la cuenta, datos de autenticación sensitivos (SAD por sus siglas en inglés), datos de titulares de tarjetas y datos PAN no son intercambiables y se utilizan deliberadamente en PCI DSS. Se ha aclarado el cuadro con los elementos más utilizados de los datos de los titulares de las tarjetas y los datos SAD, si se permite su almacenamiento, y si los datos deben hacerse ilegibles.	Aclaración u Orientación
Relación entre PCI DSS y PA-DSS	Relación entre PCI DSS y las Estándares de Software de PCI SSC	Sección redefinida acera de la relación entre PCI DSS y los estándares de software de PCI SSC, con mención de la PA-DSS (que se retira en octubre de 2022).	Requisito en Evolución
Alcance de los requisitos de PCI DSS	Alcance de los requisitos de PCI DSS	Se ha aclarado la aplicabilidad de los requisitos de PCI DSS y la definición del entorno de datos de los titulares de las tarjetas (CDE). Se han ampliado los ejemplos de componentes del sistema a los que se aplican PCI DSS; se han añadido la nube y otros componentes del sistema. Se ha añadido el diagrama "Entendiendo el Alcance de PCI DSS".	Aclaración u Orientación
Alcance de los requisitos de PCI DSS	Alcance de los Requisitos de PCI DSS: confirmación Anual del Alcance de PCI DSS	Se ha añadido un subtítulo y se ha aclarado el contenido existente.	Aclaración u Orientación

Sección		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Anexo D Segmentación y Muestreo de Instalaciones Empresariales/ Componentes del Sistema	Alcance de los Requisitos de PCI DSS: Segmentación	Se ha trasladado el diagrama de segmentación que se encontraba en el Anexo D, y se le han hecho pequeñas modificaciones. Se ha cambiado el título de la subsección y se han actualizado las referencias de "segmentación de la red" a "segmentación" para respaldar una gama de controles de segmentación más amplia.	Aclaración u Orientación
Alcance de los Requisitos de PCI DSS: Inalámbrico	Alcance de los Requisitos de PCI DSS: Inalámbrico	Se ha aclarado que la detección de redes inalámbricas clandestinas (requisito 11.2.1) debe realizarse incluso si la red inalámbrica no se utiliza en el CDE e incluso si la entidad tiene una política que prohíbe usarla.	Aclaración u Orientación
	Alcance de los Requisitos de PCI DSS: datos Cifrados del Titular de la Tarjeta e Impacto en el alcance de PCI DSS	Subsección añadida y contenido relacionado.	Aclaración u Orientación
	Alcance de los Requisitos de PCI DSS: datos cifrados del titular de la tarjeta e impacto en el alcance de PCI DSS para los proveedores de servicios externos	Subsección añadida y contenido relacionado.	Aclaración u Orientación
Alcance de los Requisitos de PCI DSS: uso de los Proveedores de Servicios Externos/Externalización	Alcance de los Requisitos de PCI DSS: Uso de los Proveedores de Servicios Externos	Cambio en el título de la subsección, se agregó nuevo contenido y se reorganizó el contenido existente bajo nuevas sub-rúbricas.	Aclaración u Orientación
Mejores Prácticas para la Implementación de PCI DSS en los Procesos Habituales.	Mejores Prácticas para la Implementación de PCI DSS en Procesos Habituales.	Se agregaron amplias guías y aclaraciones.	Aclaración u Orientación

Sección		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Para Asesores: muestreo de las Instalaciones Empresariales/ Componentes del Sistema	Para Asesores: muestreo para las Evaluaciones de PCI DSS	Sección retitulada y actualizada ampliamente con orientación adicional y aclaraciones. Se aclaró que las referencias de muestreo fueron eliminadas de los Procedimientos de Prueba para respaldar a los asesores en la selección de muestras que sean apropiadas para la población sometida a prueba.	Aclaración u Orientación
Anexo D Segmentación y Muestreo de las Instalaciones Empresariales/ Componentes del Sistema	Para Asesores: muestreo para las Evaluaciones de PCI DSS	Se trasladó el diagrama de muestreo que aparecía en el Anexo D, con pequeñas modificaciones.	Aclaración u Orientación
	Descripción de los plazos aplicados en los Requisitos de PCI DSS.	Nueva sección para aclarar las frecuencias y los plazos especificados en PCI DSS y las expectativas relacionadas. Se añadió la explicación de "cambio significativo".	Aclaración u Orientación
	Enfoques para implementar y validar PCI DSS	Nueva sección para explicar e ilustrar los dos enfoques, definido y personalizado, para implementar y validar PCI DSS.	Requisito en Evolución
Controles de Compensación	Enfoques para implementar y validar PCI DSS	Se ha trasladado el contenido a esta sección bajo el subtítulo "Enfoque Definido".	Estructura o formato
	Protección de la información Acerca de la Postura de la Entidad en Materia de Seguridad.	Nueva sección para describir cómo las entidades pueden manejar los elementos sensitivos de su evaluación de PCI DSS.	Aclaración u Orientación
	Métodos de prueba para los Requisitos PCI DSS	Nueva sección para describir los métodos de prueba utilizados en cada uno de los Procedimientos de Prueba de PCI DSS y las correspondientes actividades previstas que debe realizar el evaluador.	Aclaración u Orientación
Proceso de Evaluación PCI DSS	Proceso de Evaluación PCI DSS	Incluye pequeñas aclaraciones. Se trasladó aquí la nota que comienza con "Los requisitos de PCI DSS no se consideran vigentes...", antes bajo Requisitos detallados de PCI DSS y Procedimientos de Evaluación de la Seguridad.	Aclaración u Orientación
	Referencias Adicionales	Nueva sección que enumera las organizaciones externas referenciadas con requisitos u orientaciones de PCI DSS.	Aclaración u Orientación

Sección		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Requisitos y Procedimientos de Evaluación de Seguridad Detallados de PCI DSS	Requisitos Detallados PCI DSS y procedimientos de Prueba de Evaluación de la Seguridad	Se remplazó el contenido de la primera página de la sección por una ilustración que explica todos los elementos de la columna de Requisitos, la columna de Procedimientos de Prueba y la columna de Orientación. En la primera página de la sección se añadió una descripción de los requisitos con la leyenda "Requisitos Adicionales sólo para los proveedores de servicios". En la primera página de la sección se añadió un resumen de los anexos que incluye los requisitos adicionales de PCI DSS para diferentes tipos de entidades.	Aclaración u Orientación

4 Resumen de los Cambios Generales en los Requisitos PCI DSS

Cambios Generales Implementados en Todos los Requisitos PCI DSS	Tipo de Cambio
Se cambió el formato de las secciones generales y se añadió un resumen de las secciones al inicio de cada requisito principal.	Estructura o formato
Se actualizaron las secciones generales y se han añadido orientaciones al principio de cada sección de requisitos.	Aclaración u Orientación
Se añadieron encabezados que describen los requisitos a lo largo de cada uno de ellos para organizar y describir los requisitos que le corresponden.	Estructura o formato
Se reenumeraron los requisitos y los procedimientos de prueba y se reorganizaron los requisitos debido a la adición de encabezados de descripción de los requisitos numerados.	Estructura o formato
Se replantearon los requisitos de la directiva para que sea objetiva.	Requisito en Evolución
Se trasladaron ejemplos de los requisitos o procedimientos de prueba a la columna de orientación.	Estructura o formato
Se eliminaron las referencias al muestreo del os procedimientos de prueba.	Aclaración u Orientación
Se acortaron los procedimientos de prueba aclarando que las pruebas deben realizarse "de acuerdo con todos los elementos especificados en este requisito" para minimizar la redundancia entre los requisitos y los procedimientos de prueba.	Aclaración u Orientación
Actualización de los requisitos lingüísticos y/o de los procedimientos de prueba correspondientes para su alineación y consistencia.	Aclaración u Orientación
Mejora en los procedimientos de prueba para aclarar el nivel de validación esperado para cada requisito.	Aclaración u Orientación
Se cambió el formato de los requisitos y los procedimientos de prueba y se introdujeron pequeños cambios de redacción para facilitar la lectura; por ejemplo, se cambió el contenido de los párrafos por puntos.	Estructura o formato
Se combinaron los requisitos que tienen el mismo objetivo y se han separado los que tienen objetivos diferentes.	Estructura o formato
Se separaron los requisitos/procedimientos de prueba complejos y se eliminaron los procedimientos de prueba redundantes o que se solapaban.	Estructura o formato
Se trasladaron los elementos requeridos que sólo se incluían en los procedimientos de prueba para aclarar el requisito y facilitar el acortamiento de los procedimientos de prueba.	Aclaración u Orientación
Se reformularon y trasladaron los requisitos de políticas y procedimientos del final al principio de cada requisito principal.	Estructura o formato
Se eliminaron las notas sobre SSL/TLS temprano de las columnas de orientación para los requisitos que hacen referencia a estos protocolos específicos.	Aclaración u Orientación
Se cambió "datos de titulares de tarjetas" por "datos de la cuenta", según sea necesario, para ajustarse al uso y a la intención.	Aclaración u Orientación
Se cambió la terminología utilizada para referirse a la frecuencia en todos los requisitos de acuerdo con la *Descripción de los Plazos Utilizados en los Requisitos PCI DSS.*	Aclaración u Orientación

Cambios Generales Implementados en Todos los Requisitos PCI DSS	Tipo de Cambio
Se añadieron títulos y se reorganizó el contenido de la columna de orientación para facilitar la comprensión y fusionar información similar.	Estructura o formato

5 Cambios Adicionales por Requisito

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Requisito 1			
Requisito 1 - General		Se actualizó el título del requisito principal para reflejar el enfoque en los "controles de seguridad de la red". Se sustituyó "cortafuegos" y "enrutadores" por "controles de seguridad de la red" para dar cabida a una gama más amplia de tecnologías utilizadas para cumplir los objetivos de seguridad que tradicionalmente cumplen los cortafuegos.	Requisito en Evolución
1.1.5	1.1.2	Se sustituyó el requisito de "Descripción de grupos, funciones y responsabilidades para la gestión de los componentes de la red" por el requisito general de funciones y responsabilidades del Requisito 1.	Requisito en Evolución
1.1	1.2.1	Se redefinió un requisito "nulo" (todo el contenido apuntaba a otros requisitos) sobre la definición, implementación y mantenimiento de los estándares de configuración de las reglas de control de la seguridad de la red.	Aclaración u Orientación
1.1.1	1.2.2	Se aclaró que los cambios se gestionan de acuerdo con el proceso de control de cambios definido en el requisito 6.5.1.	Aclaración u Orientación
1.1.4		Se eliminó un requisito redundante.	Aclaración u Orientación
1.1.6	1.2.5 1.2.6	Se separó en dos requisitos para aclarar la intención de cada uno.	Aclaración u Orientación
1.1.7	1.2.7	Se aclaró la intención de revisar las configuraciones de los controles de seguridad de la red al menos una vez cada seis meses.	Aclaración u Orientación
1.2		Se eliminó el requisito "nulo" (todo el contenido apuntaba a otros requisitos).	Estructura o formato
1.2.2	1.2.8	Se aclaró la intención de asegurar los archivos de configuración.	Aclaración u Orientación
1.2.1 1.3.4	1.3.1 1.3.2	Se separó el requisito 1.2.1 en dos requisitos para aclarar la intención de cada uno. Se eliminó el Requisito 1.3.4 que era redundante.	Aclaración u Orientación
1.2.3	1.3.3	Se aclaró la intención de implementar controles de seguridad de red entre las redes inalámbricas y el CDE.	Aclaración u Orientación
1.3	1.4.1	Se redefinió un requisito "nulo" (todo el contenido apuntaba a otros requisitos). Se aclaró que la intención es implementar controles entre redes confiables y no confiables.	Aclaración u Orientación

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	**PCI DSS v4.0**		
1.3.1 1.3.2 1.3.5	1.4.2	Se fusionaron los requisitos para aclarar que la intención es restringir el tráfico entrante desde redes no confiables.	Aclaración u Orientación
1.3.6	1.4.4	Se aclaró la intención de que los componentes del sistema que almacenan datos de titulares de tarjetas no sean accesibles directamente desde redes no confiables.	Aclaración u Orientación
1.4	1.5.1	Se aclaró que la intención es implementar controles de seguridad en cualquier dispositivo informático que se conecte tanto a redes no confiables como al CDE.	Aclaración u Orientación
Requisito 2			
Requisito 2 - General		Se actualizó el título principal del requisito para reflejar que la atención se centra en las configuraciones seguras en general, y no sólo en los valores predeterminados proporcionados por el proveedor.	Aclaración u Orientación
	2.1.2	**Nuevo requisito** para las funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión 4.0*	Requisito en Evolución
2.1	2.2.2	Se aclaró que la intención es comprender si las cuentas predeterminadas de los proveedores están en uso y gestionarlas consecuentemente.	Aclaración u Orientación
2.2.1	2.2.3	Se aclaró la intención del requisito de gestionar las funciones primarias que requieren diferentes niveles de seguridad.	Aclaración u Orientación
2.2.2 2.2.5	2.2.4	Requisitos combinados para alinear los temas similares.	Estructura o formato
2.2.3	2.2.5	Se aclaró que la intención del requisito aplica *si* hay servicios, protocolos o demonios inseguros.	Aclaración u Orientación
2.1.1	2.3.1 2.3.2	Se dividió el requisito de cambiar todos los valores predeterminados de los proveedores inalámbricos en dos requisitos para aclarar el enfoque de cada uno.	Aclaración u Orientación
2.4	12.5.1	Se trasladó el requisito para alinearlo con contenido relacionado.	Estructura o formato
2.6		Se eliminó el requisito "nulo" (todo el contenido apuntaba a otros requisitos).	Estructura o formato

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Requisito 3			
Requisito 3 - General		Se actualizó el título del requisito principal para reflejar el enfoque en los datos de las cuentas.	Aclaración u Orientación
	3.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0*	Requisito en Evolución
3.1	3.2.1	**Nuevo punto de requisito** para abordar los SAD almacenados antes de la finalizar la autorización mediante la implementación de procesos, procedimientos, políticas de eliminación y de retención de datos. *Este punto es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	3.3.2	**Nuevo requisito** para cifrar los SAD que se almacenan electrónicamente antes de completar la autorización. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
3.2.a 3.2.b	3.3.3	Se añadió un requisito para orientar los procedimientos de comprobación previos para que cualquier almacenamiento de SAD por parte de los emisores esté limitado a lo que se necesita para una necesidad legítima del negocio de emisión y está protegido.	Aclaración u Orientación
3.3	3.4.1	Se aclaró que los datos del PAN se enmascaren cuando se muestren, de modo que sólo el personal con una necesidad legítima de negocio pueda ver más dígitos aparte del BIN/cuatro últimos dígitos de los datos del PAN.	Requisito en Evolución
12.3.10	3.4.2	**Nuevo requisito** para los controles técnicos que impiden la copia y/o la reubicación de datos del PAN cuando se utilizan tecnologías de acceso remoto. Ampliado desde el requisito previo 12.3.10. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
3.4	3.5.1	Se eliminó ensambladores del punto "índices de tokens y ensambladores" para hacer ilegible el PAN.	Requisito en Evolución
	3.5.1.1	**Nuevo requisito** para los hashes criptográficos con clave cuando se utiliza el hashing para hacer ilegible los datos PAN. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
	3.5.1.2	**Nuevo requisito** que indica que el cifrado a nivel de disco o de partición sólo se utilice para hacer ilegible los datos del PAN en soportes electrónicos extraíbles o, si se utiliza en soportes electrónicos no extraíbles, que estos se hagan ilegibles mediante un mecanismo que cumpla con el Requisito 3.5.1. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
3.5.1	3.6.1.1	**Nuevo punto de requisito únicamente para proveedores de servicios** para que se incluya en la descripción documentada de la arquitectura criptográfica la prohibición del uso de las mismas claves criptográficas en entornos de producción y de prueba. *Este punto es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
Requisito 4			
Requisito 4 - General		Se actualizó el título del requisito principal para reflejar el enfoque en la "criptografía robusta" para proteger las transmisiones de datos de los titulares de tarjetas.	Aclaración u Orientación
	4.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0*	Requisito en Evolución
4.1	4.2.1	**Nuevo punto de requisito** para confirmar que los certificados utilizados para las transmisiones de datos del PAN a través de redes públicas abiertas son válidos y no han caducado o han sido revocados. *Este punto es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	4.2.1.1	**Nuevo requisito** para mantener un inventario de claves y certificados de confianza. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
Requisito 5			
Requisito 5 - General		Se actualizó el título del requisito principal para reflejar el enfoque en la protección de todos los sistemas y redes contra software malicioso.	Aclaración u Orientación
		Se sustituyó el término "antivirus" por el de "antimalware" para dar cabida a una gama más amplia de tecnologías utilizadas para cumplir con los objetivos de seguridad que tradicionalmente cumplía el software antivirus.	Requisito en Evolución
	5.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	**PCI DSS v4.0**		
5.1.2	5.2.3	Se aclaró el requisito cambiando el enfoque a "componentes del sistema que no están en riesgo por programas maliciosos".	Aclaración u Orientación
	5.2.3.1	**Nuevo requisito** para definir la frecuencia de las evaluaciones periódicas de los componentes del sistema que no representan riesgo de programas maliciosos en el análisis de riesgo específico de la entidad. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
5.2	5.3.1 5.3.2 5.3.4	Se ha dividido el requisito en tres para centrar cada requisito en un área: • Mantener la solución contra programas maliciosos al día mediante actualizaciones automáticas. • Realización de escaneos periódicos y escaneos activos o en tiempo real (con una nueva opción de análisis de comportamiento continuo), • Generación de registros de auditoría por parte de la solución contra programas maliciosos.	Aclaración u Orientación
	5.3.2.1	**Nuevo requisito** para definir la frecuencia de los escaneos periódicos de programas maliciosos en el análisis de riesgo específico de la entidad. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	5.3.3	**Nuevo requisito** para una solución contra los programas maliciosos para soportes electrónicos extraíbles. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	5.4.1	**Nuevo requisito** para detectar y proteger al personal contra los ataques de phishing. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
Requisito 6			
Requisito 6 - General		Se actualizó el título del requisito principal para incluir "software" en lugar de "aplicaciones". Se aclaró que el Requisito 6 se aplica a todos los componentes del sistema, excepto al Requisito 6.2 que sólo se aplica al software personalizado y a la medida.	Aclaración u Orientación
	6.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0*	Requisito en Evolución
6.3	6.2.1	Se trasladó el requisito de desarrollar software de forma segura para alinear todo el contenido de desarrollo de software bajo el Requisito 6.2.	Estructura o formato

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
		Se sustituyó “interno y externo" por software "personalizado y a la medida". Se aclaró que este requisito se aplica a los programas informáticos desarrollados para o por la entidad para su propio uso y no aplica para programas informáticos de terceros.	Aclaración u Orientación
6.5	6.2.2	Se trasladaron los elementos del Requisito 6.5 para la formación de los desarrolladores de software a fin de alinear todo el contenido de desarrollo de software bajo el Requisito 6.2. Se aclararon los requisitos de formación para el personal de desarrollo de software.	Aclaración u Orientación
6.3.2	6.2.3 6.2.3.1	Se trasladó el requisito de revisar el software personalizado antes de su publicación para alinear todo el contenido de desarrollo de software con el Requisito 6.2. Se dividió el requisito para separar las prácticas generales de revisión del código de aquellas necesarias si se realizan revisiones manuales del código.	Aclaración u Orientación
6.5.1 6.5.10	6.2.4	Se trasladaron los requisitos para abordar las vulnerabilidades de codificación comunes a fin de alinear todo el contenido de desarrollo de software bajo el Requisito 6.2. Se combinaron los métodos para prevenir o mitigar los ataques comunes al software en un solo requisito y se generalizó el lenguaje que describe cada tipo de ataque.	Aclaración u Orientación
6.1 6.2	6.3	Se trasladaron los requisitos relacionados con la identificación de vulnerabilidades de seguridad y con la protección de los componentes frente a vulnerabilidades mediante la aplicación de actualizaciones bajo el Requisito 6.3.	Estructura o formato
6.1	6.3.1	Se añadió un punto para aclarar la aplicabilidad a las vulnerabilidades del software personalizado y a la medida de terceros.	Aclaración u Orientación
	6.3.2	**Nuevo requisito** de mantener un inventario de software personalizado y a la medida. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
6.2	6.3.3	Se cambiaron los parches de seguridad aplicables que se instalarán en el plazo de un mes desde el lanzamiento de "parches de seguridad críticos" a "parches o actualizaciones críticas o de alta seguridad."	Requisito en Evolución
6.6	6.4.1	Se trasladó el requisito de abordar las nuevas amenazas y vulnerabilidades de las aplicaciones web de cara al público bajo el Requisito 6.4.	Estructura o formato

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	**PCI DSS v4.0**		
	6.4.2	**Nuevo requisito** para desplegar una solución técnica automatizada para las aplicaciones web de cara al público que detecte y prevenga continuamente los ataques basados en la web. Este nuevo requisito elimina la opción del Requisito 6.4.1 de revisar las aplicaciones web mediante herramientas o métodos de evaluación de la vulnerabilidad de las aplicaciones, manuales o automatizados. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	6.4.3	**Nuevo requisito** para la gestión de todos los scripts de las páginas de pago que se cargan y ejecutan en el navegador del cliente. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
6.3.1 6.4 6.4.1 – 6.4.6	6.5.1 – 6.5.6	Se trasladaron y combinaron los requisitos para los cambios en los componentes del sistema bajo el Requisito 6.5.	Estructura o formato
6.4	6.5.3 6.5.4 6.5.5 6.5.6	Se eliminó el requisito de procedimientos documentados específicos y se añadieron procedimientos de prueba para verificar las políticas y los procedimientos de cada requisito relacionado.	Aclaración u Orientación
6.4.1	6.5.3	Se cambió el término "desarrollo/prueba y producción" por entornos de "producción y preproducción".	Aclaración u Orientación
6.4.2	6.5.4	Se cambió el término "desarrollo/prueba y producción" por entornos de "producción y preproducción". Se cambió el término "separación de funciones" y se ha aclaró que la separación de roles y funciones entre la producción y la preproducción tiene como objetivo proporcionar responsabilidad para que sólo se desplieguen los cambios aprobados.	Aclaración u Orientación
6.4.3	6.5.5	Se cambió el término "pruebas o desarrollo" por el de entornos de "preproducción". Se aclaró que los datos reales del PAN no se utilicen en entornos de preproducción, excepto cuando se cumplen todos los requisitos aplicables de PCI DSS.	Aclaración u Orientación
Requisito 7			
Requisito 7 - General		Se actualizó el título del requisito principal para incluir los componentes del sistema y los datos de titulares de tarjetas.	Aclaración u Orientación
	7.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	**PCI DSS v4.0**		
7.1	7.2.1 7.2.2 7.2.3	Se eliminó el requisito para procedimientos documentados específicos y se añadieron procedimientos de prueba para verificar las políticas y los procedimientos de cada requisito relacionado.	Aclaración u Orientación
7.1.1	7.2.1	El requisito aclarado se refiere a la definición de un modelo de control de acceso.	Aclaración u Orientación
7.1.2 7.1.3	7.2.2	Requisitos combinados para asignar el acceso en función de la clasificación y la función del puesto de trabajo, y los mínimos privilegios.	Estructura o formato
7.1.4	7.2.3	El requisito aclarado se refiere a la aprobación de los privilegios requeridos por parte del personal autorizado.	Aclaración u Orientación
	7.2.4	**Nuevo requisito** de revisión de todas las cuentas de usuario y privilegios de acceso relacionados. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	7.2.5	**Nuevo requisito** para la asignación y gestión de todas las cuentas de aplicaciones y cuentas de sistemas y los privilegios de acceso relacionados. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	7.2.5.1	**Nuevo requisito** de revisión de todos los accesos a través de aplicaciones y cuentas del sistema y de los privilegios de acceso relacionados. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
8.7	7.2.6	Se movió el requisito ya que se ajusta mejor al contenido del Requisito 7.	Estructura o formato
7.2		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
Requisito 8			
Requisito 8 - General		Se estandarizaron los términos “factor de autenticación” y “credenciales de autenticación”. Se eliminó "usuarios no consumidores" y se aclaró en el resumen que los requisitos no aplican a las cuentas utilizadas por los consumidores (titulares de tarjetas).	Aclaración u Orientación
		Se eliminó la nota del resumen en la cual se enumeraban los requisitos que no aplican para las cuentas de usuario con acceso a un solo número de tarjeta a la vez para facilitar una sola transacción, y se ha añadió esa nota a cada requisito relacionado.	Estructura o formato
	8.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
8.1.1	8.2.1	Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.	Aclaración u Orientación
8.5	8.2.2	Se cambió el enfoque del requisito para permitir el uso de credenciales de autenticación compartida pero sólo de forma excepcional.	Requisito en Evolución
		Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.	Aclaración u Orientación
8.5 8.5.1	8.2.2 8.2.3	Se trasladaron los requisitos de las cuentas de grupo, compartidas o genéricas y para los proveedores de servicios con acceso remoto a las instalaciones del cliente al Requisito 8.2.	Estructura o formato
8.1.8	8.2.8	Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.	Estructura o formato
8.2	8.3.1	Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.	Estructura o formato
8.1.6 8.1.7	8.3.4	Requisitos fusionados y trasladados bajo el Requisito 8.3. Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.	Estructura o formato
		Se aumentó el número de intentos de autenticación inválidos antes de bloquear un ID de usuario de seis a 10 intentos.	Requisito en Evolución
8.2.6	8.3.5	Se aclara que este requisito sólo aplica si se utilizan contraseñas/frases de paso como factor de autenticación para cumplir el Requisito 8.3.1.	Aclaración u Orientación

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
8.2.3	8.3.6	**Nuevo requisito** para aumentar la longitud de las contraseñas de una longitud mínima de siete caracteres a una longitud mínima de 12 caracteres (o si el sistema no admite 12 caracteres, una longitud mínima de ocho caracteres). *Este requisito es una buena práctica hasta el 31 de marzo de 2025.* Hasta el 31 de marzo de 2025, las contraseñas deben tener una longitud mínima de al menos siete caracteres, de acuerdo con el Requisito 8.2.3 de la versión v3.2.1. Se aclara que este requisito sólo se aplica si se utilizan contraseñas/frases de paso como factor de autenticación para cumplir el Requisito 8.3.1. Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.	Requisito en Evolución
8.2.5	8.3.7	Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción.	Estructura o formato
8.4	8.3.8	Se trasladó el contenido sobre la comunicación de las políticas y procedimientos de autenticación de usuarios al Requisito 8.3.	Estructura o formato
8.2.4	8.3.9	Se aclara que este requisito sólo se aplica si se utilizan contraseñas/frases de paso como único factor de autenticación para el acceso de usuarios (por ejemplo, en cualquier implementación de autenticación de un solo factor). Se agregó una nota indicando que este requisito no está destinado para aplicarse a las cuentas de usuario de los terminales de punto de venta que sólo tienen acceso a un número de tarjeta a la vez para facilitar una única transacción. Se agregó una nota indicando que este requisito no se aplica a las cuentas de clientes de proveedores de servicios, pero se aplica a las cuentas del personal del proveedor de servicios.	Aclaración u Orientación
8.2.4	8.3.9	Se añadió la opción de determinar el acceso a los recursos de forma automática mediante el análisis dinámico de la postura de seguridad de las cuentas, en lugar de cambiar las contraseñas/frases de paso al menos una vez cada 90 días.	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
8.2.4.b	8.3.10	Se trasladó el contenido de un antiguo procedimiento de prueba a un requisito para proveedores de servicios para que proporcionen orientación a los clientes sobre el cambio de contraseñas/frases de paso. Se añadió una nota en la que se indica que este requisito será sustituido por el Requisito 8.3.10.1 una vez que el Requisito 8.3.10.1 entre en vigor.	Estructura o formato
	8.3.10.1	**Nuevo requisito sólo para proveedores de servicios:** si las contraseñas/frases de paso son el único factor de autenticación para el acceso de sus clientes, entonces las contraseñas/frases de paso se cambian al menos una vez cada 90 días o el acceso a los recursos se determina automáticamente analizando de forma dinámica la postura de seguridad de las cuentas. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.* Se añadió una nota en la que se indica que este requisito no se aplica a las cuentas de los usuarios consumidores que acceden a la información de sus tarjetas de pago. Se añadió una nota en la cual se indica que este requisito sustituirá al Requisito 8.3.10 una vez que entre en vigor y, hasta esa fecha, los proveedores de servicios podrán cumplir con el Requisito 8.3.10 o el 8.3.10.1.	Requisito en Evolución
8.6	8.3.11	Se trasladó el requisito relacionado con factores de autenticación, tales como tokens de seguridad físicos o lógicos, tarjetas inteligentes y certificados, al Requisito 8.3.	Estructura o formato
8.3		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
	8.4.2	**Nuevo requisito** para implementar la autenticación multifactor (MFA) para todos los accesos al CDE. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.* Se añadió una nota para aclarar que el MFA es necesario para ambos tipos de acceso especificados bajo los Requisitos 8.4.2 y 8.4.3; y que la aplicación de MFA a un tipo de acceso no sustituye la necesidad de aplicar otra instancia de MFA al otro tipo de acceso.	Requisito en Evolución
	8.5.1	**Nuevo requisito** para la implementación segura de sistemas de autenticación multifactor. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
	8.6.1	**Nuevo requisito** para la gestión de las cuentas de sistemas o de aplicaciones que pueden utilizarse para el inicio de sesión interactivo. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	8.6.2	**Nuevo requisito** para evitar que contraseñas/frases de paso estén incrustadas en el código de archivos o scripts para cualquier cuenta de aplicación y sistema que pueda utilizarse para el inicio de sesión interactivo. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	8.6.3	**Nuevo requisito** para proteger contraseñas/frases de paso en las cuentas de aplicaciones y sistemas contra el uso indebido. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
8.7	7.2.6	Se cambió de lugar el requisito ya que se ajusta mejor al contenido del Requisito 7.	Estructura o formato
Requisito 9			
Requisito 9 - General		En el resumen, se aclararon las tres áreas diferenciadas que cubre el Requisito 9 (áreas sensibles, CDE e instalaciones). En todo momento se aclaró si el requisito se aplica al CDE, a las zonas sensibles o a las instalaciones.	Aclaración u Orientación
	9.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0.*	Requisito en Evolución
9.1	9.2.4	Se añadió un requisito para abordar un punto del procedimiento de prueba anterior a fin de restringir el acceso a las consolas en áreas sensibles mediante el bloqueo cuando no se utilizan.	Aclaración u Orientación
9.2	9.3.1 9.3.2	Se dividió el requisito para identificar al personal y a los visitantes en requisitos separados, Requisitos 9.3.1 y 9.3.2 respectivamente.	Estructura o formato
9.4 9.4.1 9.4.2	9.3.2	Se combinaron los requisitos para autorizar y gestionar el acceso de los visitantes conjuntamente en el Requisito 9.3.2.	Estructura o formato
9.5 9.5.1	9.4.1 9.4.1.1 9.4.1.2	Se eliminó el requisito de procedimientos para asegurar físicamente los medios de almacenamiento (9.5) y se fusionó los procedimientos en los requisitos relacionados. Se dividió el requisito para almacenar los medios de copias de seguridad en un lugar seguro y revisar la seguridad de la ubicación de las copias de seguridad sin conexión al menos cada 12 meses en 2 requisitos.	Aclaración u Orientación

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	**PCI DSS v4.0**		
9.6 9.6.1 9.6.2 9.6.3	9.4.2 9.4.3 9.4.4	Se eliminó el requisito de procedimientos para la distribución interna y externa de los medios de almacenamiento (9.6) y se fusionaron los procedimientos en los requisitos relacionados.	Aclaración u Orientación
9.7 9.7.1	9.4.5 9.4.5.1	Se eliminó el requisito de procedimientos para el control estricto sobre el almacenamiento y accesibilidad de los medios de almacenamiento (9.7) y se han fusionado los procedimientos en los requisitos relacionados. Se dividió el requisito de mantener registros de inventario de medios de almacenamiento y realizar inventarios de medios de almacenamiento anualmente en 2 requisitos.	Aclaración u Orientación
9.8 9.8.1 9.8.2	9.4.6 9.4.7	Se eliminó el requisito de procedimientos para la destrucción de los medios de almacenamiento cuando ya no se necesitan (9.8) y se han fusionado los procedimientos en los requisitos relacionados. Se aclaró que las opciones para destruir los medios de almacenamiento cuando ya no se necesitan incluyen tanto la destrucción de los soportes electrónicos como la imposibilidad de recuperar los datos de titulares de tarjetas.	Aclaración u Orientación
9.9	9.5.1	Se aclaró que el requisito se centra en los "dispositivos de punto de interacción (POI) que capturan los datos de las tarjetas de pago mediante la interacción física directa con el factor de forma de la tarjeta de pago". Se aclaró que el requisito se aplica a los dispositivos POI desplegados que se utilizan en las transacciones con tarjeta presencial.	Aclaración u Orientación
	9.5.1.2.1	**Nuevo requisito** para definir la frecuencia de las inspecciones periódicas de los dispositivos POI en función del análisis de riesgos específicos de la entidad. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
Requisito 10			
Requisito 10 - General		Se actualizó el título del requisito principal para reflejar el enfoque en los registros de auditoría, los componentes del sistema y los datos de titulares de tarjetas. Se aclaró que estos requisitos no aplican para la actividad de consumidores (titulares de tarjetas). Se ha sustituido el término "pistas de auditoría" por "registros de auditoría".	Aclaración u Orientación
	10.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
10.2		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
10.5		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
10.5.1 – 10.5.5	10.3.1 – 10.3.4	Se han trasladado los requisitos de protección de los registros de auditoría al Requisito 10.3.	Estructura o formato
10.5.3 10.5.4	10.3.3	Requisitos combinados para alinear temas similares.	Estructura o formato
10.6		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
10.6.1 – 10.6.3	10.4.1 – 10.4.3	Se han trasladado los requisitos de revisión de los registros de auditoría al Requisito 10.4.	Estructura o formato
	10.4.1.1	**Nuevo requisito** para usar mecanismos automatizados para realizar las revisiones de registros de auditoría. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	10.4.2.1	**Nuevo requisito** para que un análisis de riesgos específico defina la frecuencia de las revisiones periódicas de los registros de auditoría para todos los demás componentes del sistema (no definidos en el Requisito 10.4.1) *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
10.7	10.5.1	Se trasladó el requisito del histórico de registros de auditoría a 10.5.1.	Estructura o formato
10.4 10.4.1 – 10.4.3	10.6.1 – 10.6.3	Se trasladaron y reorganizaron los requisitos para la sincronización horaria bajo el 10.6.	Estructura o formato
10.8	10.7.1	Se trasladó el requisito de que los *proveedores de servicios* detecten, alerten y solucionen rápidamente los fallos en los sistemas de control de seguridad críticos al Requisito 10.7.1.	Estructura o formato
	10.7.2	**Nuevo requisito** para que *todas las entidades* detecten, alerten y solucionen rápidamente los fallos en los sistemas de control de seguridad críticos. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.* Este nuevo requisito se aplica a *todas las entidades, incluyendo* dos controles de seguridad críticos adicionales no incluidos en el Requisito 10.7.1 para los proveedores de servicios.	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	**PCI DSS v4.0**		
10.8.1	10.7.3	**Nuevo requisito** para responder rápidamente a los fallos de cualquier control de seguridad crítico. Para los proveedores de servicio: este es el requisito actual PCI DSS v3.2.1. Para todas las demás entidades (que no son proveedores de servicio): se trata de un nuevo requisito. *Este requisito es una mejor práctica (para los no proveedores de servicio) hasta el 31 de marzo de 2025.*	Requisito en Evolución
Requisito 11			
Requisito 11 - General		Actualización menor del título del requisito principal.	Aclaración u Orientación
	11.1.2	**Nuevo requisito** para funciones y responsabilidades. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0.*	Requisito en Evolución
11.1	11.2.1	Se aclaró que la intención del requisito es gestionar tanto los puntos de acceso inalámbricos autorizados como los no autorizados. Se aclaró que este requisito aplica incluso cuando existe una política que prohíbe el uso de la tecnología inalámbrica.	Aclaración u Orientación
	11.3.1.1	**Nuevo requisito** para gestionar el resto de las vulnerabilidades aplicables (las que no están clasificadas como de alto riesgo o críticas) encontradas durante las exploraciones internas de vulnerabilidades. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	11.3.1.2	**Nuevo requisito** para realizar escaneos internos de vulnerabilidad mediante escaneo autenticado. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
11.2.3	11.3.1.3 11.3.2.1	Se separó el requisito para realizar escaneos de vulnerabilidades internos y externos y volver a escanear después de cualquier cambio significativo, en un requisito de escaneo interno (11.3.1.3) y externo (11.3.2.1).	Estructura o formato

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
11.3	11.4.1	Se aclaró lo siguiente: • La entidad define, documenta e implementa una metodología. • Los resultados de las pruebas de penetración se conservan durante al menos 12 meses. • La metodología incluye un enfoque documentado para evaluar y abordar el riesgo que plantean las vulnerabilidades explotables y las debilidades de seguridad encontradas durante las pruebas de penetración. • El significado de las pruebas desde dentro de la red (pruebas de penetración internas) y desde fuera de la red (pruebas de penetración externas).	Aclaración u Orientación
11.3.3	11.4.4	Se aclaró que los hallazgos de las pruebas de penetración son correctos de acuerdo con la evaluación del riesgo de la entidad que representa el problema de seguridad.	Aclaración u Orientación
	11.4.7	**Nuevos requisitos para proveedores de servicios en la nube/host** para respaldar a sus clientes en las pruebas de penetración externas. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	11.5.1.1	**Nuevo requisito para proveedores de servicios** para utilizar técnicas de detección, intrusión y/o intrusión-prevención que detecten, alerten/impiden y aborden los canales de comunicación de programas maliciosos encubiertos. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	11.6.1	**Nuevo requisito** para desplegar un mecanismo de detección de cambios y manipulaciones que alerten sobre modificaciones no autorizadas en los encabezados HTTP y en el contenido de las páginas de pago que recibe el navegador del consumidor. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
11.2		Se eliminó el requisito "nulo" (todo el contenido apuntaba a otros requisitos).	Estructura o formato
11.1.2	12.10.5	Se trasladó el requisito de los procedimientos de respuesta a incidentes si se detectan puntos de acceso inalámbricos no autorizados para alinearlos con otros elementos de respuesta a incidentes.	Estructura o formato
11.5.1	12.10.5	Se trasladó el requisito de responder a las alertas generadas por la solución de detección de cambios para alinearlo con otros elementos de respuesta a incidentes.	Estructura o formato

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Requisito 12			
Requisito 12 - General		Se actualizó el título del requisito principal para reflejar que se centra en las políticas y programas organizacionales que apoyan la seguridad de la información.	Aclaración u Orientación
12.2		Se eliminó el requisito de realizar una evaluación formal de los riesgos en toda la organización y se sustituyó por el análisis de riesgos específicos (12.3.1 y 12.3.2).	Requisito en Evolución
12.4	12.1.3	Se añadió el reconocimiento formal de sus responsabilidades por parte del personal.	Requisito en Evolución
12.5 12.5.1 – 12.5.5	12.1.4	Se aclaró que las responsabilidades se asignan formalmente a un Director de Seguridad Informática o a otro miembro de la dirección ejecutiva que tiene conocimientos de seguridad de la información. Se fusionaron requisitos para asignar formalmente la responsabilidad de la seguridad de la información.	Aclaración u Orientación
12.3 12.3.1 12.3.9	12.2.1	Se aclaró que la intención del requisito es para las políticas de uso aceptable de las tecnologías para usuarios finales. Se fusionaron y eliminaron los requisitos para centrarse en la aprobación explícita de la dirección, los usos aceptables de las tecnologías y una lista de productos de hardware y software aprobados por la empresa para el uso de los empleados.	Aclaración u Orientación
12.3.10	3.4.2	Se eliminó un requisito y se agregó el nuevo Requisito 3.4.2 de controles técnicos para evitar la copia y/o la reubicación de datos PAN cuando se utilizan tecnologías de acceso remoto.	Requisito en Evolución
	12.3.1	**Nuevo requisito** para realizar un análisis de riesgo específico a cualquier requisito de PCI DSS que proporciona flexibilidad en la frecuencia con la que se realiza. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	12.3.2	**Nuevo requisito para las entidades que utilizan un Enfoque Personalizado** para desempeñar un análisis de riesgo específico para cada requisito de PCI DSS que la entidad cumple con el enfoque personalizado. *Este requisito entra en vigor inmediatamente para todas las entidades que se someten a una evaluación v4.0 y que utilizan un enfoque personalizado.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
	12.3.3	**Nuevo requisito** de documentar y revisar las secuencias de cifrado y los protocolos criptográficos en uso al menos una vez cada 12 meses. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	12.3.4	**Nuevo requisito** de revisar las tecnologías de hardware y software en uso al menos una vez cada 12 meses. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
12.11 12.11.1	12.4.2 12.4.2.1	Se trasladaron los requisitos de las revisiones para confirmar que el personal está realizando las tareas de PCI DSS de acuerdo con las políticas y los procedimientos en el Requisito 12.4, para alinearlos con otros requisitos de gestión de las actividades de cumplimiento de PCI DSS.	Estructura o formato
2.4	12.5.1	Se trasladó al Requisito 12.5 para alinearlo con otros requisitos de documentación y validación del alcance de PCI DSS.	Estructura o formato
	12.5.2	**Nuevo requisito** de documentar y confirmar el alcance de PCI DSS al menos cada 12 meses y cuando se produzcan cambios significativos en el entorno contemplado. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0*	Requisito en Evolución
	12.5.2.1	**Nuevo requisito para que los proveedores de servicios** documenten y confirmen el alcance de PCI DSS al menos una vez cada seis meses y cuando se produzcan cambios significativos en el entorno contemplado. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	12.5.3	**Nuevo requisito para los proveedores de servicios** para hacer una revisión documentada (interna) del impacto en el alcance de PCI DSS y la aplicabilidad de los controles en caso de cambios significativos en la estructura organizativa. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
12.6	12.6.1	Se aclara que la intención es que todo el personal conozca la política de seguridad de la información de la entidad y su papel en la protección de los datos de los titulares de las tarjetas.	Aclaración u Orientación
	12.6.2	**Nuevo requisito** de revisar y actualizar (según sea necesario) el programa de concienciación sobre la seguridad de la información al menos una vez cada 12 meses. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
12.6.1 12.6.2	12.6.3	Requisitos fusionados para la formación en materia de concienciación sobre la seguridad.	Estructura o formato
	12.6.3.1	**Nuevo requisito** para la formación en materia de concienciación de seguridad que incluye la concienciación ante amenazas y vulnerabilidades que podrían impactar la seguridad del CDE. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	12.6.3.2	**Nuevo requisito** de formación en materia de concienciación sobre seguridad que incluye la concientización sobre el uso aceptable de las tecnologías de usuario final, de acuerdo con el Requisito 12.2.1. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
12.8		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
12.8.1 – 12.8.5	12.8.1 – 12.8.5	Se reemplazó “Proveedor de Servicios” con Proveedor de Servicios Externos (TPSP). Se aclaró que el uso de un TPSP que cumpla con PCI DSS no hace que una entidad esté en cumplimiento con PCI DSS, ni elimina la responsabilidad de la entidad por su propio cumplimiento de PCI DSS.	Aclaración u Orientación
12.8.2	12.8.2	Se reemplazó “Proveedor de Servicios” con Proveedor de Servicios Externos (TPSP).	Aclaración u Orientación
12.8.3	12.8.3	Se reemplazó “Proveedor de Servicios” con Proveedor de Servicios Externos (TPSP).	Aclaración u Orientación
12.8.4	12.8.4	Se reemplazó “Proveedor de Servicios” con Proveedor de Servicios Externos (TPSP). Se aclaró que cuando una entidad posee un acuerdo que tiene un TPSP para cumplir con los requisitos de PCI DSS en nombre de la entidad, esta última debe trabajar con el TPSP para asegurarse de que se cumplan los requisitos de PCI DSS aplicables. Si el TPSP no cumple con los requisitos de PCI DSS aplicables, entonces, esos requisitos tampoco “están vigentes” para la entidad.	Aclaración u Orientación
12.8.5	12.8.5	Se reemplazó “Proveedor de Servicios” con Proveedor de Servicios Externos (TPSP). Se aclaró que la información sobre los requisitos de PCI DSS gestionada por el TPSP y la entidad deben incluir cualquier tipo de información compartida entre el TPSP y la entidad.	Aclaración u Orientación

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
	12.9.2	**Nuevo requisito para que los proveedores de servicios** apoyen las solicitudes de información de sus clientes en el cumplimiento de los Requisitos 12.8.4 y 12.8.5. *Este requisito entra en vigor inmediatamente para todas las evaluaciones de la versión v4.0.*	Requisito en Evolución
12.10		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
12.10.1	12.10.1	Se sustituyó "violación del sistema" y "compromiso" por "incidente de seguridad sospechoso o confirmado".	Aclaración u Orientación
12.10.3	12.10.3	Se reemplazaron las “alertas” por "incidentes de seguridad sospechosos o confirmados".	Aclaración u Orientación
12.10.4	12.10.4	Se sustituyó "violación del sistema" con "incidente de seguridad sospechoso o confirmado".	Aclaración u Orientación
	12.10.4.1	**Nuevo requisito** para realizar un análisis de riesgos específico a fin de definir la frecuencia de la capacitación periódica del personal de respuesta ante incidentes. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
12.10.5 11.1.2 11.5.1	12.10.5	Se fusionaron los requisitos y se actualizaron los sistemas de monitoreo de seguridad que se deben supervisar y atender como parte del plan de respuesta ante incidentes para incluir lo siguiente: • Detección de puntos de acceso inalámbricos no autorizados. (anteriormente 11.1.2), • Mecanismos de detección de cambios en archivos críticos. (anteriormente 11.5.1), • **Nuevo punto de requisito** para el uso de un mecanismo de detección de cambios y manipulaciones en las páginas de pago (relacionado con el nuevo requisito 11.6.1). *Este punto es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	12.10.7	**Nuevo requisito** para procedimientos de respuesta a incidentes que se iniciarán cuando se detecte que hay datos PAN almacenados en un lugar inadecuado. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Anexo A1:			
Anexo A1 - General		Se actualizaron los requisitos principales para reflejar el enfoque en los proveedores de servicios de arrendamiento múltiples. Se actualizó la visión general de los requisitos para describir a los proveedores de servicios de arrendamiento múltiples y sus entornos, y para aclarar las responsabilidades entre los proveedores de servicios de arrendamiento múltiples y sus clientes. Se actualizó "proveedor de alojamiento compartido" por "proveedor de alojamiento de usuarios múltiples".	Aclaración u Orientación
A1		Se eliminó el requisito (todo el contenido apuntaba a otros requisitos).	Estructura o formato
	A1.1.1	**Nuevo requisito** para implementar la separación lógica entre los entornos de los proveedores y los entornos de los clientes. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	A1.1.4	**Nuevo requisito** para confirmar, a través de pruebas de penetración, la eficiencia de los controles de separación lógica utilizados para separar los entornos de los clientes. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
	A1.2.3	**Nuevo requisito** para implementar los procesos o mecanismos para reportar y abordar vulnerabilidades e incidentes de seguridad de la información presuntos o confirmados. *Este requisito es una buena práctica hasta el 31 de marzo de 2025.*	Requisito en Evolución
A1.4	A1.2.2	Se reemplazó “comprometido” con "incidentes de seguridad sospechosos o confirmados".	Aclaración u Orientación
Anexo A2:			
Los únicos cambios introducidos en el Anexo A2 fueron añadir el título en la descripción del requisito A2.1 y re-enumerar los tres requisitos como A2.1.1, A2.1.2 y A2.1.3.			Aclaración u Orientación

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Anexo A3:			
Anexo A3 - General		Se aclaró que otros estándares PCI pueden hacer referencia a la ejecución de este Anexo. Se aclaró que no todos los requisitos de PCI DSS se aplican a todas las entidades que se someten a una evaluación de PCI DSS, por lo que algunos requisitos de PCI DSS se duplican en este Anexo. Cualquier pregunta acerca de este anexo debe dirigirse a los adquirentes o marcas de pago.	Aclaración u Orientación
A3.2.1	A3.2.1	Se actualizaron los elementos relacionados para el alcance de la documentación de PCI DSS y la confirmación para ajustarse al nuevo Requisito 12.5.2.	Requisito en Evolución
	A3.3.1	**Nuevo punto de requisitos** para detectar, alertar e informar sobre los fallos de los mecanismos automatizados de revisión de registros. **Nuevo punto de requisitos** para detectar, alertar e informar sobre los fallos de los códigos automatizados de revisión de herramientas. Estos puntos corresponden a las mejores prácticas hasta el 31 de marzo de 2025.	Requisito en Evolución
Anexo B: Controles de Compensación	Anexo B: Controles de Compensación	Se aclaró que los controles compensatorios pueden considerarse cuando una entidad no puede cumplir con un requisito de PCI DSS explícitamente como está escrito, debido a "limitaciones técnicas o empresariales legítimas y documentadas". Se actualizó el punto 2 para mencionar el Objetivo de Enfoque Personalizado y su uso para entender la intención de la mayoría de los requisitos de PCI DSS. Se aclaró la intención del punto 4 para abordar el riesgo adicional que supone no cumplir con el requisito de PCI DSS. Se añadió el punto 6 para aclarar que los controles compensatorios se utilizan para abordar los requisitos actuales y futuros, y no pueden utilizarse para abordar un requisito omitido en el pasado.	Aclaración u Orientación

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
Anexo C Ficha de Control de Compensación	Anexo C Ficha de Control de Compensación	Se aclaró que la intención es que la entidad utilice la hoja de trabajo para definir sus controles compensatorios. Se actualizó el punto 1 para «documentar las limitaciones técnicas o empresariales legítimas que impiden el cumplimiento del requisito original". Se reordenaron los elementos de la hoja de trabajo para mover el punto 4 al punto 2. Se actualizó el punto 3 para mencionar el Objetivo del Enfoque Personalizado, y se dividió el punto en dos partes para "Definir el objetivo del control original" e "Identificar el objetivo que cumple el control compensatorio." Se eliminó la Hoja de Control de Compensación - Ejemplo Completado. Se incluirá un ejemplo completo actualizado en un documento de orientación separado.	Aclaración u Orientación
	Anexo D Enfoque Personalizado	**Nuevo Anexo** para explicar y dar instrucciones sobre el Enfoque Personalizado.	Aclaración u Orientación
	Anexo E Muestras de Plantillas para respaldar el Enfoque Personalizado	**Nuevo Anexo** con ejemplos de plantillas para la matriz de controles y un análisis de riesgos específico que la entidad debe documentar como parte del enfoque personalizado. Se aclaró que las entidades no están obligadas a seguir los formatos específicos de las plantillas, sino que deben proporcionar toda la información definida en cada una de ellas. Incluye dos plantillas: • E1 Ejemplo de Plantilla de Matriz de Control • E2 Ejemplo de Plantilla de Análisis de Riesgo Específico.	Aclaración u Orientación
	Anexo F Aprovechamiento del Marco de Seguridad del Software de PCI para cumplir con el Requisito 6	**Nuevo Anexo** para describir cómo una entidad puede cumplir con varios elementos del Requisito 6 mediante el uso de software personalizado y a la medida que se desarrolla y mantiene de acuerdo con uno de los estándares de Software Seguro de PCI SSC.	Aclaración u Orientación

Requisito		Descripción del Cambio	Tipo de Cambio
PCI DSS v3.2.1	PCI DSS v4.0		
	Anexo G Glosario de Términos, Abreviaturas y Acrónimos de PCI DSS	**Nuevo Anexo para** el Glosario de PCI DSS v4.0. Las actualizaciones generales del Glosario incluyen que: • Se añadieron nuevos términos en función de los requisitos actualizados o de la retroalimentación recibida, • Se eliminaron los términos comunes que pueden encontrarse fácilmente en otras fuentes, • Se eliminaron los términos no utilizados en PCI DSS v4.0, • Se acortaron las definiciones de acrónimos.	Aclaración u Orientación
Anexo D Segmentación y Muestreo de Instalaciones Empresariales/Componentes del Sistema		Se eliminó el Anexo y se trasladó el contenido anterior a las secciones tituladas "Segmentación" y "Para los Evaluadores: Muestreo para Evaluaciones de PCI DSS. "	Aclaración u Orientación

6 Resumen de los Nuevos Requisitos

Como se ha indicado en la tabla anterior, los nuevos requisitos PCI DSS v4.0 son ya sea:

- Efectivos inmediatamente para todas las evaluaciones de PCI DSS v4.0.

O

- Mejores prácticas hasta el 31 de marzo de 2025.

Nuevo Requisito		Aplicable a		Entrada en Vigor	
		Todas las Entidades	Sólo Proveedores de Servicios	Inmediatamente para todas las Evaluaciones v4.0	31 de Marzo de 2025
2.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 2 están documentadas, asignadas y comprendidas.	✓		✓	
3.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 3 están documentadas, asignadas y comprendidas.	✓		✓	
3.2.1	Todo SAD almacenados antes de la finalizar la autorización se mantiene al mínimo mediante la implementación de procesos, procedimientos, políticas de eliminación y de retención de datos.	✓			✓
3.3.2	Todo SAD almacenado electrónicamente antes de completar la autorización se cifra mediante criptografía sólida	✓			✓
3.3.3	Los SAD almacenados por los emisores están cifrados mediante criptografía reforzada.		✓[1]		✓
3.4.2	Los controles técnicos que impiden copiar y/o la reubicar los datos PAN cuando se utilizan tecnologías de acceso remoto con la excepción de autorizaciones explícitas.	✓			✓
3.5.1.1	Los *hashes* utilizados para hacer ilegible 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.	✓			✓
3.5.1.2	Implementación del cifrado a nivel de disco o de partición cuando se utiliza para hacer ilegible el PAN.	✓			✓

[1] *Sólo aplica para los emisores y empresas que respaldan la emisión de servicios y almacenan datos de autenticación sensitivos.*

Nuevo Requisito		Aplicable a		Entrada en Vigor	
		Todas las Entidades	Sólo Proveedores de Servicios	Inmediatamente para todas las Evaluaciones v4.0	31 de Marzo de 2025
3.6.1.1	Una descripción documentada de la arquitectura criptográfica incluye la prevención del uso de las mismas claves criptográficas en entornos de producción y de prueba.		✓		✓
4.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 4 están documentadas, asignadas y comprendidas.	✓		✓	
4.2.1	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.	✓			✓
4.2.1.1	Se mantiene un inventario de las claves y de los certificados confiables.	✓			✓
5.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 5 están documentadas, asignadas y comprendidas.	✓		✓	
5.2.3.1	Se realiza un análisis de riesgos específico para determinar la frecuencia de las evaluaciones periódicas de los componentes del sistema identificados como libre de riesgo de programas malintencionados.	✓			✓
5.3.2.1	Se realiza un análisis de riesgo específico para determinar la frecuencia de los escaneos periódicos programas malintencionados.	✓			✓
5.3.3	Se realizan escaneos en contra de los programas maliciosos cuando se utilizan medios electrónicos extraíbles.	✓			✓
5.4.1	Se establecen los mecanismos para detectar y proteger al personal contra ataques de phishing.	✓			✓
6.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 6 están documentadas, asignadas y comprendidas.	✓		✓	

Nuevo Requisito		Aplicable a		Entrada en Vigor	
		Todas las Entidades	Sólo Proveedores de Servicios	Inmediatamente para todas las Evaluaciones v4.0	31 de Marzo de 2025
6.3.2	Mantener un inventario de software personalizado y a la medida y para facilitar la gestión de vulnerabilidades y parches.	✓			✓
6.4.2	Desplegar una solución técnica automatizada para las aplicaciones web de cara al público que detecte y prevenga continuamente los ataques basados en la web.	✓			✓
6.4.3	Gestionar todos los scripts de las páginas de pago que se cargan y ejecutan en el navegador del consumidor.	✓			✓
7.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 7 están documentadas, asignadas y comprendidas.	✓		✓	
7.2.4	Revisión de todas las cuentas de usuario y privilegios de acceso de manera apropiada.	✓			✓
7.2.5	Asignar y administrar todas las aplicaciones y cuentas del sistema y los privilegios de ingreso relacionados apropiadamente.	✓			✓
7.2.5.1	Revisar todos los ingresos por aplicación y todas las cuentas de usuario y los privilegios de acceso correspondientes.	✓			✓
8.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 8 están documentadas, asignadas y comprendidas.	✓		✓	
8.3.6	Nivel mínimo de complejidad de las contraseñas cuando se utilizan como factor de autenticación.	✓			✓
8.3.10.1	Si las contraseñas/frases de paso son el único factor de autenticación para que los usuarios del cliente ingresen, las contraseñas/frases de paso se cambian al menos cada 90 días o la postura de seguridad de las cuentas se analiza dinámicamente para determinar el ingreso a los recursos en tiempo real.		✓		✓
8.4.2	Autenticación de Factores Múltiples para todos los ingresos al CDE.	✓			✓

Nuevo Requisito		Aplicable a		Entrada en Vigor	
		Todas las Entidades	Sólo Proveedores de Servicios	Inmediatamente para todas las Evaluaciones v4.0	31 de Marzo de 2025
8.5.1	Los sistemas de autenticación multifactoriales se implementan adecuadamente.	✓			✓
8.6.1	Gestionar los inicios de sesión interactivos utilizados por los sistemas o aplicaciones.	✓			✓
8.6.2	Las contraseñas/frases de paso que se usan para el inicio de sesión interactivo para las cuentas de aplicaciones y sistemas están protegidas contra el uso indebido.	✓			✓
8.6.3	Las contraseñas/frases de acceso para cualquier aplicación y cuentas de sistema están protegidas contra el uso indebido.	✓			✓
9.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 9 están documentadas, asignadas y comprendidas.	✓		✓	
9.5.1.2.1	Se realiza un análisis de riesgo específico para determinar la frecuencia de las inspecciones periódicas de los dispositivos POI.	✓			✓
10.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 10 están documentadas, asignadas y comprendidas.	✓		✓	
10.4.1.1	Las revisiones de los registros de auditoría están automatizadas.	✓			✓
10.4.2.1	Se realiza un análisis de riesgo específico para determinar la frecuencia de las revisiones de registros para todos los demás componentes del sistema.	✓			✓
10.7.2	Las fallas de los sistemas de control de seguridad críticos se detectan, informan y atienden con prontitud.	✓			✓
10.7.3	Las fallas en los sistemas de control de seguridad críticos se atienden con prontitud.	✓			✓
11.1.2	Las funciones y responsabilidades para realizar las actividades del Requisito 11 están documentadas, asignadas y comprendidas.	✓		✓	

Nuevo Requisito		Aplicable a		Entrada en Vigor	
		Todas las Entidades	Sólo Proveedores de Servicios	Inmediatamente para todas las Evaluaciones v4.0	31 de Marzo de 2025
11.3.1.1	Se gestionan todas las otras vulnerabilidades aplicables (aquellas no clasificadas como de alto riesgo o críticas).	✓			✓
11.3.1.2	Los escaneos de vulnerabilidades internas se realizan mediante escaneos autenticados.	✓			✓
11.4.7	Los proveedores de servicios multi-inquilinos brindan respaldo a sus clientes para las pruebas de penetración externas.		✓		✓
11.5.1.1	Se abordan los canales de comunicación de programas maliciosos encubiertos, a través de técnicas de detección y/o prevención de intrusiones.		✓		✓
11.6.1	Se despliega un mecanismo de detección de cambios y manipulaciones para las páginas de pago.	✓			✓
12.3.1	Se documenta un análisis de riesgo específico para cada requisito de PCI DSS que proporcione flexibilidad para la frecuencia con que se realiza.	✓			✓
12.3.2	Se realiza un análisis de riesgo específico para cada requisito de PCI DSS que se cumpla siguiendo el enfoque personalizado.	✓		✓	
12.3.3	Se documentan y revisan las secuencias de cifrado criptográfico y los protocolos en uso.	✓			✓
12.3.4	Se revisan las tecnologías de hardware y software.	✓			✓
12.5.2	El alcance de PCI DSS se documenta y confirma al menos una vez cada 12 meses.	✓		✓	
12.5.2.1	El alcance de PCI DSS es documentado y confirmado al menos una vez cada seis meses y ante cambios significativos.		✓		✓
12.5.3	El impacto de los cambios organizacionales significativos en el alcance de PCI DSS se documenta y se revisa, y los resultados se comunican a la gerencia ejecutiva.		✓		✓

Nuevo Requisito		Aplicable a		Entrada en Vigor	
		Todas las Entidades	Sólo Proveedores de Servicios	Inmediatamente para todas las Evaluaciones v4.0	31 de Marzo de 2025
12.6.2	El programa de concienciación sobre la seguridad se revisa al menos una vez cada 12 meses y se actualiza según sea necesario.	✓			✓
12.6.3.1	La capacitación en concientización de seguridad incluye la concientización ante las amenazas que podrían impactar la seguridad del CDE, incluyendo el phishing y los ataques relacionados y la ingeniería social.	✓			✓
12.6.3.2	La capacitación en concientización en materia de seguridad incluye la concientización acerca del uso aceptable de las tecnologías de usuario final.	✓			✓
12.9.2	Los TPSP apoyan las solicitudes de los clientes para proporcionar el estado de cumplimiento de PCI DSS e información sobre los requisitos de PCI DSS que son responsabilidad del TPSP.		✓	✓	
12.10.4.1	Se desarrolla un análisis de riesgos específico a fin de definir la frecuencia de la capacitación periódica del personal de respuesta a incidentes.	✓			✓
12.10.5	El plan de respuesta a incidentes de seguridad incluye alertas del mecanismo de detección de cambios y alteraciones en las páginas de pago.	✓			✓
12.10.7	Los procedimientos de respuesta a incidentes están implementados y se inician cuando se detectan los datos PAN.	✓			✓
A1.1.1	El proveedor de servicios multiusuario confirma que el ingreso hacia y desde el entorno del cliente está lógicamente separado para evitar accesos no autorizados.		✓		✓
A1.1.4	El proveedor de servicios multiusuario confirma la efectividad de los controles de separación lógica utilizados para separar los entornos del cliente, al menos una vez cada seis meses mediante pruebas de penetración.		✓		✓

Nuevo Requisito		Aplicable a		Entrada en Vigor	
		Todas las Entidades	Sólo Proveedores de Servicios	Inmediatamente para todas las Evaluaciones v4.0	31 de Marzo de 2025
A1.2.3	El proveedor de servicios multiusuario implementa los procesos o mecanismos para informar y abordar incidentes y vulnerabilidades de seguridad sospechados o confirmados.		✓		✓
A3.3.1	Las fallas de lo siguiente son detectadas, alertadas y reportadas de manera oportuna: • Mecanismos de revisión automatizados. • Herramientas de revisión de código automatizadas.	✓			✓
Totales:		53	11	13	51
Gran Total: 64					