Norma de seguridad de datos de la **Industria de tarjetas de pago (PCI)**

Resumen de los cambios de la versión 2.0 a la 3.0 de las PCI DSS (Normas de seguridad de datos de la Industria de tarjetas de pago)

Noviembre de 2013

Introducción

Este documento proporciona un resumen de los cambios de la versión 2.0 a la versión 3.0 de las PCI DSS. La Tabla 1 proporciona una descripción general de los tipos de cambios incluidos en la versión 3.0 de las PCI DSS. La Tabla 2 proporciona un resumen de los cambios materiales que se encuentran en la versión 3.0 de las PCI DSS.

Tabla 1: Tipos de cambios

Tipo de cambio	Definición
Aclaración	Aclara el objetivo o la intención del requisito. Se asegura de que la redacción concisa de la norma exprese el objetivo deseado de los requisitos.
Guía adicional	Explicación, definición o instrucción orientada a mejorar la comprensión o proporcionar más información sobre un tema particular.
Requisito en desarrollo	Cambios para asegurar que las normas estén al día con las amenazas y los cambios emergentes del mercado.

Tabla 2: Resumen de cambios

Sección		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
Información sobre la aplicabilidad de las PCI DSS	Información sobre la aplicabilidad de las PCI DSS	Se aclaró que los SAD (datos de autenticación confidenciales) no se deben almacenar después de la autorización incluso si no hay PAN (números de cuentas principales) en el entorno.	Aclaración
Relación entre PCI DSS y PA-DSS	Relación entre PCI DSS y PA-DSS	Se aclaró que todas las aplicaciones que almacenan, procesan o transmiten datos del titular de la tarjeta están dentro del alcance para la evaluación de las PCI DSS de una entidad, incluso si las PA-DSS están validadas. Se aclaró la aplicabilidad de las PCI DSS a los proveedores de aplicaciones de pago.	Aclaración
Alcance de la evaluación del cumplimiento de los requisitos de las PCI DSS	Alcance de los requisitos de las PCI DSS	Se agregaron ejemplos de componentes del sistema y se agregó orientación sobre cómo determinar con precisión el alcance de la evaluación. Se aclaró la intención de segmentación. Se aclararon las responsabilidades del tercero y sus clientes para el alcance y la cobertura de los requisitos de las PCI DSS, y se aclaró la evidencia que se espera que los terceros proporcionen a sus clientes para que puedan verificar el alcance de la evaluación de las PCI DSS del tercero.	Guía adicional
	Implementación de las PCI DSS en los procesos habituales	Se creó una nueva sección para proporcionar orientación sobre los “procesos habituales” para implementar la seguridad en este tipo de actividades a fin de mantener el cumplimiento continuo con las PCI DSS. Tenga en cuenta que esta sección incluye solamente recomendaciones y orientación, no nuevos requisitos de las PCI DSS.	Guía adicional
	Procedimientos de evaluación	Se agregó un nuevo encabezado para separar la sección del alcance de las PCI DSS de la sección de muestreo.	Aclaración
Muestreo de instalaciones de la empresa/componentes del sistema	Para los asesores: Muestreo de instalaciones de la empresa/componentes del sistema	Se mejoró la orientación sobre el muestreo para asesores.	Guía adicional
Instrucciones y contenido del informe de cumplimiento	Instrucciones y contenido del informe de cumplimiento	Se reubicó el contenido anterior para separar los documentos: plantilla para crear informes ROC (informes sobre cumplimiento) de las PCI DSS e instrucciones para crear informes ROC (informes sobre cumplimiento) de las PCI DSS.	Aclaración
Cumplimiento de las PCI DSS: Pasos para completar el proceso	Proceso de evaluación de las PCI DSS	Se actualizó la sección para hacer hincapié en el proceso de evaluación, en lugar de en la documentación.	Aclaración

Requisitos Requisitos de las PCI DSS y Procedimientos de evaluación de la seguridad	Requisitos Requisitos de las PCI DSS y Procedimientos de evaluación de la seguridad	Al inicio de esta sección, se agregó información para definir los encabezados de las columnas de esta sección y se eliminaron las referencias de las columnas “Implementado”, “No implementado” y “Fecha objetivo/Comentarios”.	Aclaración

Cambios generales implementados en todos los requisitos de las PCI DSS	Tipo
Se agregó una nueva columna para describir la intención de cada requisito, con contenido proveniente del documento anterior sobre orientación para la Navegación de las PCI DSS. La orientación de esta columna tiene la intención de ayudar a comprender los requisitos y no reemplaza ni extiende los procedimientos de pruebas ni los requisitos de las PCI DSS.	Guía adicional
Para las políticas de seguridad y los procedimientos operativos diarios (anteriormente, requisitos 12.1.1 y 12.2), se asignó un nuevo número de requisito y se trasladaron los requisitos y los procedimientos de pruebas en cada uno de los requisitos del 1 al 11.	Aclaración
Se actualizó la redacción sobre requisitos y los procedimientos de pruebas correspondientes para obtener alineación y uniformidad.	Aclaración
Se separaron los requisitos y los procedimientos de pruebas complejos para lograr claridad, y se eliminaron los procedimientos de pruebas redundantes o superpuestos.	Aclaración
Se mejoraron los procedimientos de pruebas para aclarar el nivel de validación esperado para cada requisito.	Aclaración
Otros cambios de edición general incluyen los siguientes: • Se eliminaron las siguientes columnas: “Implementado”, “No implementado” y “Fecha objetivo/Comentarios”. • Se enumeraron nuevamente los requisitos y los procedimientos de pruebas para adaptarlos a los cambios. • Se volvió a dar formato a los requisitos y los procedimientos de pruebas por cuestiones de legibilidad; p. ej., para el contenido de párrafos, se usó un formato con viñetas, etc. • Se implementaron cambios menores en todo el texto por cuestiones de legibilidad. • Se corrigieron errores tipográficos.	

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	PCI DSS, versión 3.0		
Requisito 1			
1.1.x	1.1.x	Se aclaró que se deben documentar e implementar las normas de firewalls y routers.	Aclaración
1.1.2	1.1.2 1.1.3	Se aclaró lo que debe incluir el diagrama de red y se agregó un nuevo requisito en 1.1.3 para un diagrama actual que muestre los flujos de datos del titular de la tarjeta.	Requisito en desarrollo
1.1.5	1.1.6	Se aclararon los ejemplos de servicios, protocolos y puertos inseguros para especificar las versiones 1 y 2 del SNMP (protocolo simple de administración de red).	Aclaración
1.2.2	1.2.2	Se aclaró que la intención de proteger los archivos de configuración del router es impedir el acceso no autorizado.	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
1.2.3	1.2.3	Se aclaró que la intención del control del tráfico entre las redes inalámbricas y el CDE (entorno de los datos del titular de la tarjeta) es “permitir únicamente el tráfico autorizado”.	Aclaración
1.3.4	1.3.4	Se aclaró que la intención del requisito es que se implementen medidas antisuplantación para detectar las direcciones IP de origen falsificadas y bloquear su ingreso en la red.	Aclaración
1.4	1.4	Se alineó el texto entre el requisito y los procedimientos de pruebas para lograr uniformidad.	Aclaración
Requisito 2			
2.1	2.1	Se aclaró que el requisito para cambiar las contraseñas predeterminadas de los proveedores se aplica a todas las contraseñas predeterminadas, lo que incluye sistemas, aplicaciones, software de seguridad, terminales, etc., y que se eliminen o desactiven todas las cuentas predeterminadas innecesarias.	Aclaración
2.1.1	2.1.1	Se aclaró que la intención del requisito es que, durante la instalación, se modifiquen los valores predeterminados de todos los proveedores inalámbricos.	Aclaración
2.2	2.2	Se aclaró que las normas de configuración del sistema incluyen procedimientos para cambiar todos los valores predeterminados proporcionados por el proveedor y las cuentas predeterminadas innecesarias.	Aclaración
2.2.2	2.2.2 2.2.3	Se dividió el requisito 2.2.2 en dos para hacer hincapié de manera separada en los puertos, los protocolos y los servicios *necesarios* (2.2.2) y en los puertos, protocolos y servicios *seguros* (2.2.3).	Aclaración
	2.4	Se creó un nuevo requisito para mantener un inventario de los componentes del sistema que se encuentran dentro del alcance de las PCI DSS a fin de respaldar el desarrollo de las normas de configuración.	Requisito en desarrollo
Requisito 3			
3.1 3.1.1	3.1	Se combinaron el requisito 3.1.1 y los procedimientos de pruebas en el requisito 3.1 para aclarar y reducir la redundancia.	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
3.2	3.2	Se aclaró que, ante la recepción de datos de autenticación confidenciales, se deben convertir en irrecuperables tras completar el proceso de autorización. Se aclararon los procedimientos de pruebas para las empresas que respaldan los servicios de emisión y almacenan datos de autenticación confidenciales.	Aclaración
3.3	3.3	Se aclaró la intención del requisito para ocultar el PAN (número de cuenta principal) mediante la consolidación de la nota anterior en el cuerpo del requisito y la mejora de los procedimientos de pruebas.	Aclaración
3.4.1	3.4.1	Se aclaró que el acceso lógico para el cifrado de disco se debe administrar de manera *separada* e independiente de los mecanismos de acceso de control y *autenticación* del sistema operativo nativo, y que las claves de cifrado no deben estar *asociadas a* cuentas de usuarios.	Aclaración
3.5	3.5	Se aclaró que se deben implementar y documentar procedimientos de administración de claves.	Aclaración
3.5.2	3.5.2 3.5.3	Se dividió el requisito 3.5.2 en dos para hacer hincapié por separado en el almacenamiento de claves criptográficas de manera segura (3.5.2) y en la menor cantidad de ubicaciones posibles (3.5.3). El requisito 3.5.2 también proporciona flexibilidad con más opciones para el almacenamiento seguro de claves criptográficas.	Aclaración
3.6.x	3.6.x	Se agregaron procedimientos de pruebas para verificar la implementación de procedimientos de administración de claves criptográficas.	Aclaración
3.6.6	3.6.6	Se aclararon los principios de conocimiento dividido y control doble.	Aclaración
Requisito 4			
4.1	4.1	Se alineó el texto entre el requisito y los procedimientos de pruebas para lograr uniformidad. También se expandieron los ejemplos de redes públicas y abiertas.	Aclaración
Requisito 5			
Requisito 5: general		Se actualizó el título para reflejar la intención del requisito (*proteger todos los sistemas contra malware).*	Aclaración
	5.1.2	Se creó un nuevo requisito para evaluar las amenazas futuras de malware para cualquier sistema que no se considere frecuentemente afectado por software malicioso.	Requisito en desarrollo

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
5.2	5.2	Se alineó el texto entre el requisito y los procedimientos de pruebas para lograr uniformidad.	Aclaración
	5.3	Se creó un nuevo requisito para garantizar que las soluciones de antivirus se ejecuten de manera activa (anteriormente, en 5.2) y que los usuarios no puedan desactivarlas ni alterarlas, a menos que estén específicamente autorizados por la gerencia según el caso.	Requisito en desarrollo
Requisito 6			
6.2	6.1	Se cambió el orden de los requisitos 6.1 y 6.2. El requisito 6.1 ahora tiene la finalidad de identificación y clasificación de riesgos de las nuevas vulnerabilidades y el 6.2 dispone la instalación de parches en caso de vulnerabilidades críticas. Se aclaró cómo se alinea el proceso de clasificación de riesgos (6.1) con el proceso de instalación de parches (6.2).	Aclaración
6.1	6.2	Consulte la explicación anterior del requisito 6.1. Además, se aclaró que este requisito se aplica a los parches “correspondientes”.	Aclaración
6.3	6.3	Se agregó una nota para aclarar que el requisito de los procesos de desarrollo de software por escrito se aplica a todo el software de desarrollo interno y el software personalizado.	Aclaración
6.3.1	6.3.1	Se cambió “producción previa” por “desarrollo/prueba” para aclarar la intención del requisito.	Aclaración
6.4	6.4	Se mejoraron los procedimientos de pruebas para incluir las revisiones de documentos para todos los requisitos desde 6.4.1 hasta 6.4.4.	Aclaración
6.4.1	6.4.1	Se alineó el texto entre los requisitos y los procedimientos de pruebas para aclarar que la separación de los entornos de producción/desarrollo se impone mediante controles de acceso.	Aclaración
6.5	6.5	Se actualizó la capacitación de los desarrolladores para incluir los modos de evitar vulnerabilidades de codificación comunes y para comprender cómo se manejan los datos confidenciales en la memoria.	Aclaración
6.5.x	6.5.x	Se actualizaron los requisitos para reflejar las vulnerabilidades de codificación actuales y emergentes, y garantizar las pautas de codificación. Se actualizaron los procedimientos de pruebas para aclarar cómo las técnicas de codificación abordan las vulnerabilidades.	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
	6.5.10	Se creó un nuevo requisito para prácticas de codificación para proteger ante una autenticación y administración de sesión interrumpidas. *En vigor a partir del 1 de julio de 2015.*	Requisito en desarrollo
6.6	6.6	Se aumentó la flexibilidad mediante la especificación de una *solución técnica automatizada que detecte y prevenga los ataques basados en la web* en lugar de un "firewall de aplicación web". Se agregó una nota para aclarar que esta evaluación no es la misma que los análisis de vulnerabilidad que se exigen en el requisito 11.2.	Aclaración
Requisito 7			
7.1	7.1	Se volvió a redactar el procedimiento de pruebas para aclarar lo que abarca la política, en función de los cambios en los requisitos del 7.1.1 al 7.1.4.	Aclaración
	7.1.1	Se creó un nuevo requisito 7.1.1 para cubrir la definición de necesidades de acceso para cada función, a fin de respaldar los requisitos del 7.1.2 al 7.1.4.	Aclaración
7.1.1	7.1.2	Se volvió a orientar el requisito sobre la limitación de las ID de los usuarios privilegiados a la menor cantidad de privilegios necesarios, y se mejoraron los procedimientos de pruebas.	Aclaración
7.1.2	7.1.3	Se volvió a orientar el requisito sobre la asignación del acceso según la función y la clasificación del puesto de las personas.	Aclaración
7.1.4		Se eliminó el requisito 7.1.4 anterior (cubierto en el requisito 7.2).	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
Requisito 8			
Requisito 8: general		Se actualizó el título para reflejar la intención del requisito (identificar y autenticar todo el acceso a los componentes del sistema). Se actualizaron y reorganizaron los requisitos para proporcionar un enfoque más holístico a la identificación y la autenticación del usuario: • El requisito 8.1 se centró en la identificación del usuario. • El requisito 8.2 se centró en la autenticación del usuario. • Se actualizaron los requisitos para considerar métodos de autenticación que no sean contraseñas. • Se cambió de "contraseñas" a "contraseñas/frases" en los casos en que el requisito solo se aplica a contraseñas/frases. • Se cambió de "contraseñas" a "credenciales de autenticación" en los casos en que el requisito se aplica a cualquier tipo de credencial de autenticación. • Se aclaró que los requisitos de seguridad de las contraseñas se aplican a las cuentas usadas por proveedores terceros.	Aclaración
8.5.6	8.1.5	Se aclaró que el requisito para el acceso de proveedores remotos se aplica a los proveedores que acceden, respaldan o mantienen los componentes del sistema, y que esto se debe desactivar cuando no está en uso.	Aclaración
8.4.2	8.2.1	Se aclaró que se debe usar una criptografía segura para que las credenciales de autenticación queden ilegibles durante la transmisión y el almacenamiento.	Aclaración
8.5.2	8.2.2	Se aclaró que se debe verificar la identificación del usuario antes de modificar las credenciales de autenticación, y se agregaron la entrega de nuevos tokens y la generación de nuevas claves como ejemplos de modificaciones.	Aclaración
8.5.10 8.5.11	8.2.3	Se combinaron los requisitos mínimos de seguridad y solidez de la contraseña en un único requisito, y se aumentó la flexibilidad para las alternativas que cumplen con las mismas condiciones de solidez y seguridad.	Requisito en desarrollo
8.3	8.3	Se aclaró que el requisito de autenticación de dos factores se aplica a los usuarios, los administradores y todos los terceros, lo que incluye el acceso de proveedores para soporte o mantenimiento.	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
8.5.7	8.4	Se mejoró el requisito para incluir orientación sobre la documentación y la comunicación para indicar cómo deben proteger los usuarios sus credenciales de autenticación, lo que incluye la reutilización y el cambio de contraseñas/frases si se sospecha que están en riesgo.	Aclaración
	8.5.1	Se creó un nuevo requisito para los proveedores de servicios con acceso remoto a las instalaciones del cliente para usar credenciales de autenticación exclusivas para cada cliente. *En vigor a partir del 1 de julio de 2015.*	Requisito en desarrollo
	8.6	Se creó un nuevo requisito en el que se usan otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.) diferentes de los mecanismos que se deben vincular con la cuenta de una persona y garantiza que solo el usuario previsto pueda obtener acceso con ese mecanismo.	Requisito en desarrollo
8.5.16	8.7	Se alineó el texto entre el requisito y los procedimientos de pruebas para lograr uniformidad.	Aclaración
Requisito 9			
9.1.2	9.1.2	Se aclaró que la intención del requisito es implementar controles de acceso físico o lógico para proteger las conexiones de red de acceso público.	Aclaración
9.2.x	9.2.x	Se aclaró que la intención del requisito es identificar y otorgar acceso a los visitantes y el personal del sitio, y establecer distinciones entre estos, y que las placas de identificación son solo una opción (no son obligatorias).	Aclaración
	9.3	Se creó un nuevo requisito para controlar el acceso físico a áreas confidenciales para el personal del sitio, lo que incluye un proceso para autorizar el acceso y revocar el acceso inmediatamente después de la finalización.	Requisito en desarrollo
9.3.x	9.4.x	Se alineó el texto entre el requisito y los procedimientos de prueba para lograr uniformidad y para aclarar que se debe acompañar a los visitantes en todo momento, y que la pista de auditoría sobre la actividad de los visitantes debe incluir el acceso a las instalaciones, la sala de informática o el centro de datos.	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
9.5 – 9.10	9.5 – 9.8	El requisito 9.6 anterior se trasladó y volvió a enumerar como 9.5, y el requisito 9.5 anterior se volvió a enumerar como subrequisito 9.5.1. El requisito 9.7 anterior se volvió a enumerar como 9.6, y el requisito 9.8 anterior se volvió a enumerar como subrequisito 9.6.3. El requisito 9.9 anterior se volvió a enumerar como 9.7, y el requisito 9.10 anterior se volvió a enumerar como requisito 9.8.	Aclaración
	9.9.x	Se incorporaron nuevos requisitos para proteger contra alteración y sustitución a los dispositivos que capturan datos de la tarjeta de pago a través de interacción física directa con la tarjeta. *En vigor a partir del 1 de julio de 2015.*	Requisito en desarrollo
Requisito 10			
10.1	10.1	Se aclaró que se deberían implementar pistas de auditoría para vincular el acceso a los componentes del sistema con cada persona, en lugar de solo establecer un proceso.	Aclaración
10.2.1	10.2.1	Se aclaró que el propósito es que el acceso de todos los *usuarios* a los datos del titular de la tarjeta se incluyan en las pistas de auditoría.	Aclaración
10.2.5	10.2.5	Se mejoró el requisito para incluir cambios en los mecanismos de identificación y autenticación (lo que incluye la creación de nuevas cuentas, la mejora de privilegios), y todos los cambios, incorporaciones y eliminaciones a las cuentas con acceso administrativo o de raíz.	Requisito en desarrollo
10.2.6	10.2.6	Se mejoró el requisito para incluir la detención o la pausa de los registros de auditoría.	Requisito en desarrollo
10.6	10.6.x	Se aclaró que la intención de las revisiones de los registros es identificar anomalías o actividad sospechosa, y se proporcionó más orientación sobre el alcance de las revisiones de registros diarios. También se permitió mayor flexibilidad para la revisión de los eventos de seguridad y los registros de sistemas críticos a diario y otros registros de eventos de manera periódica, según lo define la estrategia de gestión de riesgos de la entidad.	Aclaración
Requisito 11			

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
11.1.x	11.1.x	Se mejoró el requisito para incluir un inventario de puntos de acceso inalámbrico autorizados y una justificación de negocio (11.1.1) para respaldar el análisis de dispositivos inalámbricos no autorizados, y se agregó un nuevo requisito 11.1.2 para que coincida con el procedimiento de pruebas ya existente, para los procedimientos de respuesta ante incidentes si se detectan puntos de acceso inalámbrico no autorizados.	Requisito en desarrollo
11.2	11.2	Se agregó orientación sobre la combinación de informes de varios análisis para archivar y documentar un resultado aprobado.	Guía adicional
11.2.1	11.2.1	Se aclaró que los análisis internos cuatrimestrales de vulnerabilidades incluyen la segunda realización de los análisis, según sea necesario, hasta que se resuelvan todas las vulnerabilidades “altas” (según se identifican en el requisito 6.1 de las PCI DSS), y deben estar a cargo de personal calificado.	Aclaración
11.2.2	11.2.2	Se aclaró que los análisis externos de vulnerabilidades incluyen una segunda realización de los análisis, según sea necesario, hasta que se logren análisis aprobados, y se agregó una nota para hacer referencia a la Guía del programa del ASV (proveedor aprobado de escaneo).	Aclaración
11.2.3	11.2.3	Se aclaró que los análisis internos y externos realizados tras cambios significativos incluyen la segunda realización de los análisis, según sea necesario, hasta que se resuelvan todas las vulnerabilidades “altas” (según se identifican en el requisito 6.1 de las PCI DSS), y deben estar a cargo de personal calificado.	Aclaración
	11.3	Se creó un nuevo requisito para implementar una metodología para las pruebas de penetración. *En vigor a partir del 1 de julio de 2015. Hasta la implementación de la versión 3.0, se deben seguir los requisitos de la versión 2.0 de las PCI DSS para las pruebas de penetración.*	Requisito en desarrollo
11.3	11.3.1 11.3.2	Se dividió el requisito 11.3 anterior en el requisito 11.3.1 para los requisitos de las pruebas de penetración *externas* y en el requisito 11.3.2 para los requisitos de las pruebas de penetración *internas*.	Aclaración
11.3	11.3.3	Se creó un nuevo requisito a partir del procedimiento de pruebas anterior (11.3.b) para corregir las vulnerabilidades detectadas encontradas durante las pruebas de penetración y para repetir las pruebas a fin de verificar las correcciones.	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
	11.3.4	Se creó un nuevo requisito, si se usa la segmentación para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes, para realizar pruebas de penetración a fin de verificar que los métodos de segmentación sean operativos y efectivos.	Requisito en desarrollo
11.4	11.4	Se aumentó la flexibilidad mediante la especificación de *técnicas de prevención de intrusión-detección o intrusión para detectar o prevenir intrusiones en la red* en lugar de "sistemas de intrusión-detección o sistemas de intrusión-prevención".	Aclaración
11.5	11.5	Se aumentó la flexibilidad mediante la especificación del *mecanismo de detección de cambios* en lugar de la "monitorización de integridad de archivos".	Aclaración
	11.5.1	Se creó un nuevo requisito para implementar un proceso para responder ante cualquier alerta generada por el mecanismo de detección de cambios (respalda al requisito 11.5).	Requisito en desarrollo
Requisito 12			
12.1.1 12.2	1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6	Se combinaron los requisitos anteriores en 12.1.1 (para que la política de seguridad de la información aborde todos los requisitos de las PCI DSS) y 12.2 (para los procedimientos de seguridad operativa), y se los trasladó a los Requisitos del 1 al 11, según el requisito de cada uno.	Aclaración
12.1.3	12.1.1	El requisito 12.1.3 anterior se trasladó al 12.1.1.	Aclaración
12.1.2	12.2	El requisito 12.1.2 anterior se trasladó al 12.2 para un proceso de evaluación de riesgos anual, y se aclaró que la evaluación de riesgos se debe realizar, al menos, una vez al año *y después de cambios significativos en el entorno*.	Requisito en desarrollo
12.3.4	12.3.4	Se aclaró que el "etiquetado" es un ejemplo de un método que se puede utilizar.	Aclaración
12.3.8	12.3.8	Se implementó un nuevo procedimiento de pruebas para verificar la política a fin de desconectar las sesiones de acceso remoto tras un período específico de inactividad.	Aclaración
12.3.10	12.3.10	Se alineó el texto entre el requisito y los procedimientos de pruebas para clarificar que, cuando hay una necesidad comercial autorizada para que el personal acceda a los datos del titular de la tarjeta mediante tecnologías de acceso remoto, los datos se deben proteger de conformidad con todos los requisitos de las PCI DSS correspondientes.	Aclaración

Requisito		Cambio	Tipo
PCI DSS, versión 2.0	**PCI DSS, versión 3.0**		
12.8	12.8	Se aclaró la intención de implementar y mantener las políticas y los procedimientos para administrar a los proveedores de servicios con quienes se comparten los datos del titular de la tarjeta o que podrían afectar la seguridad de los datos del titular de la tarjeta.	Aclaración
12.8.2	12.8.2	Se aclararon las responsabilidades correspondientes para el reconocimiento/acuerdo escrito del proveedor de servicios.	Aclaración
	12.8.5	Se creó un nuevo requisito para mantener información sobre qué requisitos de las PCI DSS administra cada proveedor de servicios, y cuáles están a cargo de la entidad.	Requisito en desarrollo
	12.9	Se creó un nuevo requisito para que los proveedores de servicios proporcionen el reconocimiento/acuerdo escrito a sus clientes, tal como se especifica en el requisito 12.8. *En vigor a partir del 1 de julio de 2015.*	Requisito en desarrollo
12.9.x	12.10.x	Se volvió a enumerar el requisito y se actualizó el 12.10.5 para aclarar que la intención es incluir alertas de los *sistemas de monitorización de seguridad* en el plan de respuesta ante incidentes.	Aclaración