El Enfoque Prioritario para Lograr el Cumplimiento de la PCI DSS

La Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) proporciona una estructura detallada de 12 Requisitos para proteger los datos del titular de la tarjeta que son almacenados, procesados y/o transmitidos por los comerciantes y otras organizaciones. Por su carácter integral, la norma proporciona una gran cantidad de información acerca de la seguridad - tanta que algunas personas que son responsables de la seguridad de los datos del titular de la tarjeta pueden preguntarse por dónde empezar el viaje permanente del cumplimiento. Con este fin, el Consejo de Normas de Seguridad de la PCI ofrece el siguiente Enfoque Priorizado para ayudar a las partes interesadas a entender dónde pueden actuar para reducir el riesgo más temprano en el proceso de cumplimiento. Ningún hito único en el Enfoque Priorizado proporcionará la seguridad integral o el cumplimiento de la PCI DSS, pero seguir sus directrices ayudará a las partes interesadas a acelerar el proceso de asegurar los datos del titular de la tarjeta.

ASPECTOS DESTACADOS

Puede ayudar a los comerciantes a identificar los más altos objetivos de riesgo

Crea un lenguaje común en torno a los esfuerzos de implementación y evaluación de la PCI DSS

Los hitos permiten a los comerciantes demostrar el progreso sobre el proceso de cumplimiento

¿Qué es el Enfoque Priorizado?

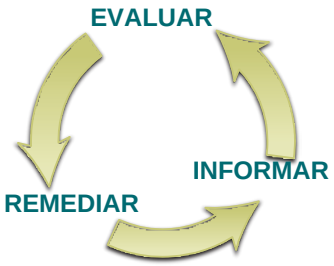
El Enfoque Priorizado ofrece seis hitos de seguridad que ayudarán a los comerciantes y a otras organizaciones de manera incremental a protegerse contra los más altos factores de riesgo y las crecientes amenazas mientras recorren el camino hacia el cumplimiento de la PCI DSS. El Enfoque Priorizado y sus hitos (que se describen en la página 2) están destinados a proporcionar los siguientes beneficios:

- Una hoja de ruta que una organización puede utilizar para hacer frente a sus riesgos en orden de prioridad
- Un enfoque pragmático que permita las “victorias rápidas”
- Soporta la planificación financiera y operativa
- Promueve indicadores de progreso objetivos y medibles
- Ayuda a promover la consistencia entre los asesores

Objetivos del Enfoque Priorizado

El Enfoque Priorizado proporciona una hoja de ruta de las actividades de cumplimiento basada en el riesgo asociado con el almacenamiento, el procesamiento y/o la transmisión de los datos del titular de la tarjeta. La hoja de ruta ayuda a priorizar los esfuerzos para lograr el cumplimiento, establecer hitos, disminuir el riesgo de infracciones a los datos del titular de la tarjeta más pronto en el proceso de cumplimiento, y ayuda a los adquirentes a medir objetivamente las actividades de cumplimiento y la reducción del riesgo de los comerciantes, los proveedores de servicios, y otros. El Enfoque Priorizado se ideó después de factorizar los datos de las infracciones reales, y la retroalimentación de los Asesores de Seguridad Certificados, los investigadores forenses, y la Junta de asesores del Consejo de Normas de Seguridad de la PCI. No pretende sustituir, crear un atajo o salir del paso del enfoque hacia el cumplimiento de la PCI DSS, ni tampoco es un marco obligatorio estándar aplicable a todas las organizaciones. El Enfoque Priorizado es adecuado para los comerciantes que se someten a una evaluación in situ o que utilizan SAQ D.

EL CUMPLIMIENTO DE LA PCI DSS ES UN PROCESO CONTINUO



FUNDADORES DEL PCI SSC

ORGANIZACIONES PARTICIPANTES

Comerciantes, bancos, procesadores, desarrolladores y proveedores en puntos de venta

Descargo

Para lograr el cumplimiento de la PCI DSS, una organización debe cumplir todos los requisitos de la PCI DSS, independientemente del orden en que se cumplen o si la organización que solicita el cumplimiento sigue el Enfoque Priorizado de la PCI DSS. Este documento no modifica ni resume la PCI DSS o algunos de sus requisitos, y puede ser modificado sin previo aviso.
El PCI SSC no es responsable de los errores o daños de cualquier tipo que puedan resultar del uso de la información contenida en el presente documento. El PCI SSC no ofrece ningún aval, garantía o representación alguna en cuanto a la información proporcionada en este documento, y no asume responsabilidad alguna respecto al uso o mal uso de dicha información.

Hitos para Priorizar los Esfuerzos de Cumplimiento de la PCI DSS

El Enfoque Priorizado incluye seis hitos. La matriz siguiente resume los objetivos de alto nivel y las intenciones de cada hito. El resto de este documento asigna los hitos a cada uno de los doce requisitos de la PCI DSS y sus subrequisitos.

Hitos	Objetivos
1	**Eliminar los datos confidenciales de autenticación y limitar la retención de los datos.** Este hito se dirige a un área clave de riesgo para las entidades que han estado en riesgo. Recuerde - si no se almacenan los datos confidenciales de autenticación y otros datos del titular de la tarjeta, se reducirán considerablemente los efectos del riesgo. Si no los necesita, no los almacene
2	**Proteja los sistemas y las redes, y esté preparado para responder a una falla en el sistema.** Este hito se dirige a los controles de los puntos de acceso para la mayoría de riesgos, y los procesos para responder.
3	**Aplicaciones seguras de tarjetas de pago.** Este hito se dirige a los controles de las aplicaciones, los procesos de la aplicación y los servidores de la aplicación. Las deficiencias en estas áreas ofrecen una presa fácil para poner en riesgo a los sistemas y obtener acceso a los datos del titular de la tarjeta.
4	**Supervisar y controlar el acceso a sus sistemas.** Los controles para este hito le permiten detectar quién, qué, cuándo y cómo con respecto a quién accede a su entorno de red y de datos del titular de la tarjeta.
5	**Proteja los datos del titular de la tarjeta que fueron almacenados.** Para aquellas organizaciones que han analizado sus procesos comerciales y que determinaron que deben almacenar los Números de Cuenta Primarios, el Hito Cinco se dirige a los mecanismos de protección clave para esos datos almacenados.
6	**Finalice los esfuerzos de cumplimiento restantes, y asegúrese de que todos los controles están implementados.** La intención del Hito Seis es completar los requisitos de la PCI DSS, y finalizar todas las políticas relacionadas restantes, los procedimientos y los procesos necesarios para proteger el entorno de los datos del titular de la tarjeta.

Requisitos de la PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta						
1.1 Establezca e implemente normas de configuración para firewalls y routers que incluyan lo siguiente:						
1.1.1 Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers						6
1.1.2 Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.	1					
1.1.3 El diagrama actual que muestra todos los flujos de datos de titulares de tarjetas entre los sistemas y las redes.	1					
1.1.4 Requisitos para tener un firewall en cada conexión a Internet y entre cualquier DMZ (zona desmilitarizada) y la zona de la red interna.		2				
1.1.5 Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.						6
1.1.6 Documentación y justificación de negocio para el uso de todos los servicios, protocolos y puertos permitidos, incluida la documentación de las funciones de seguridad implementadas en aquellos protocolos que se consideran inseguros.		2				
1.1.7 Requisito de la revisión de las normas de firewalls y routers, al menos, cada seis meses.						6
1.2 Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas. *Nota: Una "red no confiable" es toda red externa a las redes que pertenecen a la entidad en evaluación o que excede la capacidad de control o administración de la entidad.*						
1.2.1 Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.		2				
1.2.2 Asegure y sincronice los archivos de configuración de routers.		2				
1.2.3 Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos firewalls para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.		2				
1.3 Prohíba el acceso público directo entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.						
1.3.1 Implemente una DMZ (zona desmilitarizada) para limitar el tráfico entrante solo a aquellos componentes del sistema que proporcionan servicios, protocolos y puertos con acceso público autorizado.		2				
1.3.2 Restrinja el tráfico entrante de Internet a las direcciones IP dentro de la DMZ.		2				
1.3.3 Implementar medidas antisuplantación para detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red. (Por ejemplo, bloquear el tráfico proveniente de Internet con una dirección de fuente interna).		2				
1.3.4 No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet.		2				
1.3.5 Solo permita conexiones "establecidas" en la red.		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
1.3.6 Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.		2				
1.3.7 No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas. *Nota: Entre los métodos para ocultar direcciones IP, se pueden incluir, a modo de ejemplo, los siguientes:* • *Traducción de Dirección de Red (NAT)* • *Ubicación de los servidores que contengan datos del titular de la tarjeta detrás de los servidores proxy/firewalls.* • *Eliminación o filtrado de anuncios de enrutamiento para redes privadas que emplean direcciones registradas,* • *Uso interno del espacio de direcciones RFC1918 en lugar de direcciones registradas.*		2				
1.4 Instale software de firewall personal o una funcionalidad equivalente en todos los dispositivos móviles (de propiedad de la compañía y/o de los trabajadores) que tengan conexión a Internet cuando están fuera de la red (por ejemplo, computadoras portátiles que usan los trabajadores), y que también se usan para acceder al CDE. Las configuraciones de firewall (o equivalente) incluyen: • Se definen los ajustes específicos de configuración. • El firewall personal (o funcionalidad equivalente) está en ejecución activa. • El firewall personal (o una funcionalidad equivalente) no es alterable por los usuarios de los dispositivos informáticos portátiles.		2				
1.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.		2				
Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad						
2.1 Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red. Esto rige para TODAS las contraseñas predeterminadas, por ejemplo, entre otras, las utilizadas por los sistemas operativos, los software que prestan servicios de seguridad, las cuentas de aplicaciones y sistemas, los terminales de POS (puntos de venta), las aplicaciones de pago, las cadenas comunitarias de SNMP (protocolo simple de administración de red), etc.		2				
2.1.1 En el caso de entornos inalámbricos que están conectados al entorno de datos del titular de la tarjeta o que transmiten datos del titular de la tarjeta, cambie TODOS los valores predeterminados proporcionados por los proveedores de tecnología inalámbrica al momento de la instalación, incluidas, a modo de ejemplo, las claves de cifrado inalámbricas predeterminadas, las contraseñas y las cadenas comunitarias SNMP (protocolo simple de administración de red).		2				
2.2 Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria. Entre las fuentes de normas de alta seguridad aceptadas en la industria, se pueden incluir, a modo de ejemplo: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).			3			

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
2.2.1 Implemente sólo una función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor. (Por ejemplo, los servidores web, servidores de base de datos y DNS se deben implementar en servidores separados). *Nota: Cuando se utilicen tecnologías de virtualización, implemente solo una función principal por componente de sistema virtual.*			3			
2.2.2 Habilite solo los servicios, protocolos y daemons, etc., necesarios, según lo requiera la función del sistema.			3			
2.2.3 Implementar funciones de seguridad adicionales para los servicios, protocolos o daemons requeridos que no se consideren seguros. *Nota: Cuando se utiliza la SSL/TLS temprana, se debe completar los requisitos establecidos en el Anexo A2.*		2				
2.2.4 Configure los parámetros de seguridad del sistema para evitar el uso indebido.			3			
2.2.5 Elimine todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.			3			
2.3 Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. *Nota: Cuando se utiliza la SSL/TLS temprana, se debe completar los requisitos establecidos en el Anexo A2.*		2				
2.4 Lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS.		2				
2.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.		2				
2.6 Los proveedores de hosting compartido deben proteger el entorno y los datos del titular de la tarjeta que aloja la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el Anexo A1: Requisitos adicionales de la PCI DSS para los proveedores de hosting.			3			
Requisito 3: Proteger los datos almacenados del titular de la tarjeta						
3.1 Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos que incluyan, al menos, las siguientes opciones para el almacenamiento de CHD (datos del titular de la tarjeta): • Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio • Requisitos de retención específicos para datos de titulares de tarjetas • Procesos para eliminar datos de manera cuando ya no se necesiten • Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta al acenados que excedan la retención definida.	1					
3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos de autenticación confidenciales, convierta todos los datos en irrecuperables al finalizar el proceso de autorización. Es posible que los emisores de tarjetas y las empresas que respaldan los servicios de emisión almacenen datos de autenticación si: • Si existe una justificación de negocio. • Si los datos se almacenan de forma segura. Los datos confidenciales de autenticación incluyen los datos mencionados en los requisitos 3.2.1 a 3.2.3, establecidos a continuación:	1					

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
3.2.1 No almacene contenido completo de ninguna pista (de la banda magnética ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo) después de la autorización. Estos datos se denominan alternativamente, pista completa, pista, pista 1, pista 2 y datos de banda magnética. Nota: En el transcurso normal de los negocios, es posible que se deban retener los siguientes elementos de datos de la banda magnética: • El nombre del titular de la tarjeta • Número de cuenta principal (PAN) • Fecha de vencimiento • Código de servicio Para minimizar el riesgo, almacene solamente los elementos de datos que sean necesarios para el negocio.	1					
3.2.2 No almacene el valor o código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago que se utiliza para verificar las transacciones de tarjetas ausentes) después de la autorización.	1					
3.2.3 Después de la autorización, no almacene el PIN (número de identificación personal) ni el bloqueo de PIN cifrado.	1					
3.3 Enmascare el PAN (número de cuenta principal) cuando aparezca (los primeros seis o los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis o los últimos cuatro dígitos del PAN. *Nota: Este requisito no reemplaza los requisitos más estrictos implementados para la presentación de los datos del titular de la tarjeta (por ejemplo, requisitos legales o de las marcas de las tarjetas de pago para los recibos de POS [puntos de venta]).*					5	
3.4 Convierta el PAN (número de cuenta principal) en ilegible en cualquier lugar donde se almacene (incluidos los datos que se almacenen en medios digitales portátiles, medios de copia de seguridad, y en registros) utilizando cualquiera de los siguientes enfoques: • Valores hash de una vía basados en criptografía sólida (el hash debe ser del PAN completo) • Truncamiento (los valores hash no se pueden usar para reemplazar el segmento truncado del PAN) • Tokens y ensambladores de índices (los ensambladores se deben almacenar de manera segura). • Criptografía sólida con procesos y procedimientos asociados para la administración de claves. *Nota: Para una persona malintencionada sería relativamente fácil reconstruir el PAN original si tiene acceso tanto a la versión truncada como a la versión en valores hash de un PAN. Si el entorno de una entidad tiene versiones en valores hash y truncadas del mismo PAN, se deben implementar controles adicionales para asegurar que las versiones en valores hash y truncadas no se puedan correlacionar para reconstruir el PAN original.*					5	
3.4.1 Si se utiliza el cifrado de disco (en lugar de un cifrado de base de datos por archivo o columna), se debe administrar un acceso lógico independiente y por separado de los mecanismos de autenticación y control de acceso del sistema operativo nativo (por ejemplo, no se deben utilizar bases de datos de cuentas de usuarios locales ni credenciales generales de inicio de sesión de la red). Las claves de descifrado no deben estar asociadas con las cuentas de usuarios. *Nota: Este requisito se aplica adicionalmente a todos los demás requisitos de cifrado y de gestión de claves de la PCI DSS.*					5	
3.5 Documente e implemente procedimientos que protejan las claves utilizadas para proteger los datos del titular de la tarjeta almacenados contra su posible divulgación o uso indebido: *Nota: Este requisito también se aplica a las claves utilizadas para cifrar los datos del titular de la tarjeta almacenados y para las claves de cifrado de claves utilizadas para proteger las claves de cifrado de datos; dichas claves de cifrado de claves deben ser, al menos, tan seguras como las claves de cifrado de datos.*						

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
3.5.1 Requisitos adicionales solo para los proveedores de servicios: Mantenga una descripción documentada de la arquitectura criptográfica que incluye: • Detalles de todos los algoritmos, protocolos y claves utilizados para la protección de los datos del titular de la tarjeta, incluidas la complejidad de la clave y la fecha de caducidad • Descripción del uso de la clave para cada tecla. • Inventario de un HSM SMS y otros SCD utilizados para la gestión de claves *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*					5	
3.5.2 Restrinja el acceso a las claves criptográficas a la menor cantidad de custodios necesarios.					5	
3.5.3 Siempre guarde las claves secretas y privadas utilizadas para cifrar/descifrar los datos del titular de la tarjeta en una (o más) de las siguientes formas: • Cifradas con una clave de cifrado de claves que sea, al menos, tan sólida como la clave de cifrado de datos y que se almacene separada de la clave de cifrado de datos. • Dentro de un dispositivo seguro criptográfico (como un HSM [módulo de seguridad de host] o un dispositivo de punto de interacción aprobado para la PTS). • Como, al menos, dos claves o componentes de la clave completos de acuerdo con los métodos aceptados por la industria. *Nota: No es necesario guardar las claves públicas de esta manera.*					5	
3.5.4 Guarde las claves criptográficas en la menor cantidad de ubicaciones posibles.					5	
3.6 Documente por completo e implemente todos los procesos y procedimientos de administración de claves de las claves criptográficas que se utilizan para el cifrado de datos del titular de la tarjeta, incluso lo siguiente: *Nota: Varias normas de la industria relativas a la administración de claves están disponibles en distintos recursos incluido NIST, que puede encontrar en http://csrc.nist.gov.*						
3.6.1 Generación de claves de cifrado sólido					5	
3.6.2 Distribución segura de claves de cifrado					5	
3.6.3 Almacenamiento seguro de claves de cifrado					5	
3.6.4 La clave criptográfica cambia en el caso de las claves que han llegado al final de su período de cifrado (por ejemplo, después que haya transcurrido un período definido y/o después que cierta cantidad de texto cifrado haya sido producido por una clave dada), según lo defina el proveedor de la aplicación relacionada o el responsable de las claves, y basándose en las mejores prácticas y recomendaciones de la industria (por ejemplo, NIST Special Publication 800-57).					5	
3.6.5 Retiro o reemplazo de claves (por ejemplo, mediante archivo, destrucción o revocación) según se considere necesario cuando se haya debilitado la integridad de la clave (por ejemplo, salida de la empresa de un empleado con conocimiento de una clave en texto claro, etc.) o cuando se sospeche que las claves están en riesgo. Nota: Si es necesario retener las claves de cifrado retiradas o reemplazadas, éstas se deben archivar de forma segura (por ejemplo, utilizando una clave de cifrado de claves). Las claves criptográficas archivadas se deben utilizar solo con fines de descrifrado o verificación.					5	

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
3.6.6 Si se usan operaciones manuales de administración de claves criptográficas de texto claro, se deben realizar con control doble y conocimiento dividido. Nota: Los ejemplos de operaciones manuales de administración de claves incluyen, entre otros, generación, transmisión, carga, almacenamiento y destrucción de claves.					5	
3.6.7 Prevención de sustitución no autorizada de claves criptográficas.					5	
3.6.8 Requisito para que los custodios de claves criptográficas declaren, formalmente, que comprenden y aceptan su responsabilidad como custodios de claves.					5	
3.7 ¿Las políticas de seguridad y los procedimientos operativos para la protección de los datos de titulares de tarjetas almacenados se documentan, están en uso, y son conocidas por todas las partes afectadas?					5	
Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas						
4.1 Utilizar criptografía sólida y protocolos de seguridad para proteger los datos del titular de la tarjeta confidenciales durante la transmisión por redes públicas abiertas, como por ejemplo, las siguientes: • Solo se aceptan claves y certificados de confianza. • El protocolo implementado solo admite configuraciones o versiones seguras. • La solidez del cifrado es la adecuada para la metodología de cifrado que se utiliza. *Nota: Cuando se utiliza la SSL/TLS temprana, se debe completar los requisitos establecidos en el Anexo A2.* *Ejemplos de redes públicas abiertas incluyen, entre otras, las siguientes:* • *La Internet* • *Tecnologías inalámbricas, incluso 802.11 y Bluetooth* • *Tecnología celular, por ejemplo, GSM (sistema global de comunicación móviles), CDMA (acceso múltiple por división de código)* • *Servicio de radio paquete general (GPRS)* • *Comunicaciones satelitales*		2				
4.1.1 Asegúrese de que las redes inalámbricas que transmiten los datos del titular de la tarjeta o que están conectadas al entorno de datos del titular de la tarjeta utilicen las mejores prácticas de la industria a fin de implementar un cifrado sólido para la transmisión y la autenticación.		2				
4.2 Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, SMS, el chat, etc.)		2				
4.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.		2				
Requisito 5: Utilizar y actualizar con regularidad los programas o software antivirus						
5.1 Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).		2				
5.1.1 Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.		2				
5.1.2 Para aquellos sistemas que no suelen verse afectados por software maliciosos, lleve a cabo evaluaciones periódicas para identificar y evaluar las amenazas de malware que pueden aparecer a fin de determinar si es necesario o no implementar un software antivirus en dichos sistemas.		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
5.2 Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: • Estén actualizados. • Ejecuten análisis periódicos. • Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS.		2				
5.3 Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado. *Nota: Las soluciones de antivirus se pueden desactivar temporalmente, pero solo si existe una necesidad técnica legítima como en el caso de la autorización de la gerencia en casos particulares. Si es necesario desactivar la protección de antivirus por un motivo específico, se debe contar con una autorización formal. Es posible que sea necesario implementar medidas de seguridad adicionales en el período en que no esté activa la protección de antivirus.*		2				
5.4 Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.		2				
Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros						
6.1 Establezca un proceso para identificar las vulnerabilidades de seguridad por medio de fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad, y asigne una clasificación de riesgo (por ejemplo, “alto”, “medio” o “bajo”) a las vulnerabilidades de seguridad recientemente descubiertas. *Nota: Las clasificaciones de riesgo se deben basar en las mejores prácticas de la industria y en el posible impacto. Por ejemplo, en los criterios para clasificar las vulnerabilidades, se puede tener en cuenta la puntuación base CVSS, la clasificación del proveedor o el tipo de sistema afectado.* *Los métodos para evaluar las vulnerabilidades y asignar las clasificaciones de riesgo varían según el entorno y la estrategia de evaluación de riesgos de la organización. Las clasificaciones de riesgo deben identificar, mínimamente, todas las vulnerabilidades que se consideren de “alto riesgo” para el entorno. Además de la clasificación de riesgos, las vulnerabilidades se pueden considerar críticas si suponen una amenaza inminente para el entorno, si afectan los sistemas o si generan un posible riesgo si no se contemplan. Algunos ejemplos de sistemas críticos son los sistemas de seguridad, los dispositivos y sistemas públicos, las bases de datos y otros sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta.*			3			
6.2 Asegúrese de que todos los software y componentes del sistema tengan instalados parches de seguridad proporcionados por los proveedores que ofrecen protección contra vulnerabilidades conocidas. Instale los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento. *Nota: Los parches de seguridad críticos se deben identificar de conformidad con el proceso de clasificación de riesgos definido en el Requisito 6.1.*			3			
6.3 Desarrolle aplicaciones de software internas y externas (incluso acceso administrativo a aplicaciones basado en web) de manera segura y de la siguiente manera: • De acuerdo con las PCI DSS (por ejemplo, autenticación y registros seguros). • Basadas en las normas o en las mejores prácticas de la industria. • Incorporación de seguridad de la información en todo el ciclo de vida de desarrollo del software. *Nota: Esto rige para todos los software desarrollados internamente y para todos los software personalizados desarrollados externamente.*			3			
6.3.1 Elimine las cuentas de desarrollo, de prueba y de aplicaciones personalizadas, las ID de usuario y las contraseñas antes de que las aplicaciones se activen o se pongan a disposición de los clientes.			3			

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
6.3.2 Revise el código personalizado antes de enviarlo a producción o de ponerlo a disposición de los clientes a fin de identificar posibles vulnerabilidades en la codificación (mediante procesos manuales o automáticos) y que incluya, al menos, lo siguiente: • La revisión de los cambios en los códigos está a cargo de personas que no hayan creado el código y que tengan conocimiento de técnicas de revisión de código y prácticas de codificación segura. • Las revisiones de los códigos deben garantizar que el código se desarrolle de acuerdo con las directrices de codificación segura. • Las correcciones pertinentes se implementan antes del lanzamiento. • La gerencia revisa y aprueba los resultados de la revisión de códigos antes del lanzamiento. *Nota: Este requisito de revisión de códigos se aplica a todos los códigos personalizados (tanto internos como públicos) como parte del ciclo de vida de desarrollo del sistema. Las revisiones de los códigos pueden ser realizadas por terceros o por personal interno con conocimiento. Las aplicaciones web también están sujetas a controles adicionales a los efectos de tratar las amenazas continuas y vulnerabilidades después de la implementación, conforme al Requisito 6.6 de las PCI DSS.*			**3**			
6.4 Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema. Los procesos deben incluir lo siguiente:			**3**			
6.4.1 Separe los entornos de desarrollo/prueba de los entornos de producción y refuerce la separación con controles de acceso.			**3**			
6.4.2 Separación de funciones entre desarrollo/prueba y entornos de producción			**3**			
6.4.3 Los datos de producción (PAN activos) no se utilizan para las pruebas ni para el desarrollo			**3**			
6.4.4 Eliminación de datos y cuentas de los componentes del sistema antes de que se activen los sistemas de producción			**3**			
6.4.5 Los procedimientos de control de cambios deben incluir lo siguiente:						**6**
6.4.5.1 Documentación de incidencia.						**6**
6.4.5.2 Aprobación de cambio documentada por las partes autorizadas.						**6**
6.4.5.3 Verifique que se hayan realizado las pruebas de funcionalidad y que el cambio no impacte negativamente en la seguridad del sistema.						**6**
6.4.5.4 Procedimientos de desinstalación.						**6**
6.4.6 Al término de un cambio significativo, deben implementarse todos los requisitos pertinentes de la PCI DSS en todos los sistemas y redes nuevos o modificados, y la documentación actualizada según sea el caso. *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*						**6**
6.5 Aborde las vulnerabilidades de codificación comunes en los procesos de desarrollo de software de la siguiente manera: • Capacite a los desarrolladores, por lo menos anualmente, en las técnicas actualizadas de codificación segura, incluida la forma de evitar las vulnerabilidades de codificación comunes. • Desarrolle aplicaciones basadas en directrices de codificación seguras. *Nota: Las vulnerabilidades que se enumeran desde el punto 6.5.1 hasta el 6.5.10 eran congruentes con las mejores prácticas de la industria al momento de la publicación de esta versión de las PCI DSS. Sin embargo, debido a que las mejores prácticas de la industria para la gestión de vulnerabilidades se actualizan (por ejemplo, OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), se deben utilizar las mejores prácticas actuales para estos requisitos.*			**3**			
Nota: Los Requisitos 6.5.1 al 6.5.6, que se describen a continuación, rigen para todas las aplicaciones de pago (internas o externas).						

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
6.5.1 Errores de inyección, en especial, errores de inyección SQL. También considere los errores de inyección de comandos de OS, LDAP y Xpath, así como otros errores de inyección.			3			
6.5.2 Desbordamiento de buffer			3			
6.5.3 Almacenamiento cifrado inseguro			3			
6.5.4 Comunicaciones inseguras			3			
6.5.5 Manejo inadecuado de errores			3			
6.5.6 Todas las vulnerabilidades de “alto riesgo” detectadas en el proceso de identificación de vulnerabilidades (según lo definido en el Requisito 6.1 de las PCI DSS).			3			
Nota: Los Requisitos 6.5.7 al 6.5.10, que siguen a continuación, rigen para las aplicaciones web y las interfaces de las aplicaciones (internas o externas):						
6.5.7 Lenguaje de comandos entre distintos sitios (XSS)			3			
6.5.8 Control de acceso inapropiado (como referencias no seguras a objetos directos, no restricción de acceso a URL y exposición completa de los directorios, y la no restricción de acceso a las funciones por parte de los usuarios).			3			
6.5.9 Falsificación de solicitudes entre distintos sitios (CSRF)			3			
6.5.10 Autenticación y administración de sesión interrumpidas			3			
6.6 En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente y asegúrese de que estas aplicaciones se protejan contra ataques conocidos con alguno de los siguientes métodos: • Controlar las aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, por lo menos, anualmente y después de cada cambio *Nota: Esta evaluación no es la misma que el análisis de vulnerabilidades realizado en el Requisito 11.2.* • Instalación de una solución técnica automática que detecte y prevenga ataques web (por ejemplo, firewall de aplicación web) delante de aplicaciones web públicas a fin de controlar el tráfico continuamente.			3			
6.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.			3			
Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.						
7.1 Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso.						
7.1.1 Defina las necesidades de acceso de cada función, incluso lo siguiente: • Los componentes del sistema y los recursos de datos que necesita cada función para acceder a fin de realizar su trabajo. • Nivel de privilegio necesario (por ejemplo, usuario, administrador, etc.) para acceder a los recursos.				4		
7.1.2 Limite el acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo.				4		
7.1.3 Asigne el acceso según la tarea, la clasificación y la función del personal.				4		

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
7.1.4 Solicite la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios.				4		
7.2 Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de conocer y que se configure para "negar todo", salvo que se permita específicamente. Este sistema de control de acceso debe incluir lo siguiente:						
7.2.1 Cobertura de todos los componentes del sistema				4		
7.2.2 La asignación de privilegios a una persona se basa en la clasificación del trabajo y su función.				4		
7.2.3 Configuración predeterminada de "negar todos".				4		
7.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.				4		
Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora						
8.1 Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema de la siguiente manera:						
8.1.1 Asigne a todos los usuarios una ID exclusiva antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.		2				
8.1.2 Controle la incorporación, la eliminación y la modificación de las ID de usuario, las credenciales y otros objetos de identificación.		2				
8.1.3 Cancele de inmediato el acceso a cualquier usuario cesante.		2				
8.1.4 Elimine o inhabilite las cuentas de usuario inactivas, al menos, cada 90 días.		2				
8.1.5 Administre las ID que usan los terceros para acceder, respaldar o mantener los componentes del sistema de manera remota de la siguiente manera: • Se deben habilitar solamente durante el tiempo que se necesitan e inhabilitar cuando no se usan. • Se deben monitorear mientras se usan.		2				
8.1.6 Limite los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos.		2				
8.1.7 Establezca la duración del bloqueo a un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario.		2				
8.1.8 Si alguna sesión estuvo inactiva durante más de 15 minutos, solicite al usuario que vuelva a escribir la contraseña para activar la terminal o la sesión nuevamente.		2				
8.2 Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar todos los usuarios: • Algo que el usuario sepa, como una contraseña o frase de seguridad • Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente • Algo que el usuario sea, como un rasgo biométrico.		2				
8.2.1 Deje ilegibles todas las credenciales de autenticación (como contraseñas/frases) durante la transmisión y el almacenamiento en todos los componentes del sistema mediante una criptografía sólida.		2				
8.2.2 Verifique la identidad del usuario antes de modificar alguna credencial de autenticación, por ejemplo, restablezca la contraseña, entregue nuevos tokens o genere nuevas claves.		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
8.2.3 Las contraseñas/frases deben tener lo siguiente: • Una longitud mínima de siete caracteres. • Combinación de caracteres numéricos y alfabéticos. De manera alternativa, la contraseña/frase debe tener una complejidad y una solidez, al menos, equivalente a los parámetros que se especifican anteriormente.		2				
8.2.4 Cambie la contraseña/frase de usuario, al menos, cada 90 días.		2				
8.2.5 No permita que una persona envíe una contraseña/frase nueva que sea igual a cualquiera de las últimas cuatro contraseñas/frases utilizadas.		2				
8.2.6 Configure la primera contraseña/frase y las restablecidas en un valor único para cada usuario y cámbiela de inmediato después del primer uso.		2				
8.3 Asegure todo el acceso administrativo individual que no sea de consola y todo el acceso remoto al CDE mediante la autenticación de múltiples factores. *Nota: La autenticación de múltiples factores requiere que se utilicen dos de los tres métodos de autenticación (consulte el Requisito 8.2 para obtener una descripción de los métodos de autenticación). El uso de un mismo factor dos veces (por ejemplo, utilizar dos contraseñas individuales) no se considera una autenticación de múltiples factores.*						
8.3.1 Incorporar la autenticación de múltiples factores para todo acceso que no sea de consola en el CDE para el personal con acceso administrativo. *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*		2				
8.3.2 Incorpore la autenticación de múltiples factores para todo acceso remoto que se origine desde fuera de la red de la entidad (tanto para usuarios como administradores, e incluso para todos los terceros involucrados en el soporte o mantenimiento).		2				
8.4 Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios que incluye lo siguiente: • Lineamientos sobre cómo seleccionar credenciales de autenticación sólidas. • Lineamientos sobre cómo los usuarios deben proteger las credenciales de autenticación. • Instrucciones para no seleccionar contraseñas utilizadas anteriormente. • Instrucciones para cambiar contraseñas si se sospecha que la contraseña corre riesgos.				4		
8.5 No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación de la siguiente manera: • Las ID de usuario genéricas se deben desactivar o eliminar. • No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas. • Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema.				4		
8.5.1 Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios que tengan acceso a las instalaciones del cliente (por ejemplo, para tareas de soporte de los sistemas de POS o de los servidores) deben usar una credencial de autenticación exclusiva (como una contraseña/frase) para cada cliente. *Nota: El objetivo de este requisito no es aplicarlo a los proveedores de servicios de hosting compartido que acceden a su propio entorno de hosting, donde se alojan numerosos entornos de clientes.*		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
8.6 Si se utilizan otros mecanismos de autenticación (por ejemplo, tokens de seguridad físicos o lógicos, tarjetas inteligentes, certificados, etc.), el uso de estos mecanismos se debe asignar de la siguiente manera: • Los mecanismos de autenticación se deben asignar a una sola cuenta y no compartirlos entre varias. • Se deben implementar controles físicos y lógicos para garantizar que solo la cuenta deseada usa esos mecanismos para acceder.				4		
8.7 Se restringen todos los accesos a cualquier base de datos que contenga datos del titular de la tarjeta (que incluye acceso por parte de aplicaciones, administradores y todos los otros usuarios) de la siguiente manera: • Todo acceso, consultas y acciones de usuario en las bases de datos se realizan, únicamente, mediante métodos programáticos. • Solo los administradores de la base de datos pueden acceder directamente a las bases de datos o realizar consultas en estas. • Solo las aplicaciones pueden usar las ID de aplicaciones para las aplicaciones de base de datos (no las pueden usar los usuarios ni otros procesos que no pertenezcan a la aplicación).				4		
8.8 Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.				4		
Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.						
9.1 Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.		2				
9.1.1 Utilice cámaras de video u otros mecanismos de control de acceso (o ambos) para supervisar el acceso físico de personas a áreas confidenciales. Revise los datos recopilados y correlaciónelos con otras entradas. Guárdelos durante al menos tres meses, a menos que la ley estipule lo contrario. *Nota: "Áreas confidenciales" hace referencia a cualquier centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan procesos o transmitan datos de titulares de tarjetas. No se incluyen las áreas públicas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.*		2				
9.1.2 Implemente controles físicos o lógicos para restringir el acceso a conexiones de red de acceso público. Por ejemplo, las conexiones de red en áreas públicas y en las que pueden acceder los visitantes se pueden inhabilitar y habilitar solo cuando el acceso a la red se autoriza explícitamente. De forma alternativa, se pueden implementar procesos para asegurarse de que los visitantes estén acompañados en todo momento en áreas con conexiones de red activas.		2				
9.1.3 Limite el acceso físico a los puntos de acceso inalámbricos, gateways, dispositivos manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.		2				
9.2 Desarrolle procedimientos que permitan distinguir, fácilmente, a los empleados y a los visitantes, de la siguiente manera: • Identificar empleados o visitantes nuevos (por ejemplo, mediante la asignación de placas). • Cambios en los requisitos de acceso. • Revocar las identificaciones de empleados cesantes y las identificaciones vencidas de visitantes (p. ej., placas de identificación).					5	
9.3 Controle el acceso físico de los empleados a las áreas confidenciales de la siguiente manera: • El acceso se debe autorizar y basar en el trabajo de cada persona. • El acceso se debe cancelar inmediatamente después de finalizar el trabajo, y todos los mecanismos de acceso físico, como claves, tarjetas de acceso, se deben devolver o desactivar.		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
9.4 Implemente procedimientos para identificar y autorizar a los visitantes. Los procedimientos deben incluir lo siguiente:						
9.4.1 Los visitantes reciben autorización antes de ingresar en las áreas de procesamiento o almacenamiento de los datos del titular de la tarjeta y estarán acompañados en todo momento.					5	
9.4.2 Se identifican los visitantes y se les entrega una placa u otro elemento de identificación con fecha de vencimiento y que permite diferenciar claramente entre empleados y visitantes.					5	
9.4.3 Los visitantes deben entregar la placa o la identificación antes de salir de las instalaciones o al momento del vencimiento.					5	
9.4.4 Se usa un registro de visitantes para llevar una pista de auditoría física de la actividad de los visitantes en las instalaciones, en las salas de informática y en los centros de datos donde se almacenan o se transmiten los datos del titular de la tarjeta. Documente el nombre del visitante, la empresa a la que representa y el empleado que autoriza el acceso físico en el registro. Conserve este registro durante tres meses como mínimo, a menos que la ley estipule lo contrario.					5	
9.5 Proteja físicamente todos los medios.					5	
9.5.1 Almacene los medios de copias de seguridad en un lugar seguro, preferentemente, en un lugar externo a la empresa, como un centro alternativo o para copias de seguridad, o en un centro de almacenamiento comercial. Revise la seguridad de dicho lugar una vez al año como mínimo.					5	
9.6 Lleve un control estricto de la distribución interna o externa de todos los tipos de medios y realice lo siguiente:						
9.6.1 Clasifique los medios para poder determinar la confidencialidad de los datos.					5	
9.6.2 Envíe los medios por correo seguro u otro método de envío que se pueda rastrear con precisión.					5	
9.6.3 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que se trasladen desde un área segura (incluso, cuando se distribuyen los medios a personas).					5	
9.7 Lleve un control estricto del almacenamiento y la accesibilidad de los medios.						
9.7.1 Lleve un registro detallado del inventario de todos los medios y lleve a cabo inventarios de los medios, al menos, una vez al año.					5	
9.8 Destruya los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales de la siguiente manera:						
9.8.1 Corte en tiras, incinere o convierta en pulpa los materiales de copias en papel para que no se puedan reconstruir los datos del titular de la tarjeta. Proteja los contenedores de almacenamiento destinados a los materiales que se destruirán.	1					
9.8.2 Controle que los datos del titular de la tarjeta guardados en medios electrónicos sean irrecuperables para que no se puedan reconstruir.	1					
9.9 Proteja los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones. *Nota: Estos requisitos rigen para los dispositivos de lectura de tarjetas que se usan en transacciones (es decir, al pasar o deslizar la tarjeta) en los puntos de venta. El objetivo de este requisito no es aplicarlo a los componentes de ingreso de claves, como teclados de computadoras y teclados numéricos de POS (puntos de ventas).*						
9.9.1 Lleve una lista actualizada de los dispositivos. La lista debe incluir lo siguiente: • Marca y modelo del dispositivo • Ubicación del dispositivo (por ejemplo, la dirección de la empresa o de la instalación donde se encuentra el dispositivo) • Número de serie del dispositivo u otro método de identificación única		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
9.9.2 Inspeccione periódicamente la superficie de los dispositivos para detectar alteraciones (por ejemplo, incorporación de componentes de duplicación de datos en el dispositivo) o sustituciones (por ejemplo, controle el número de serie u otras características del dispositivo para verificar que no se haya cambiado por un dispositivo fraudulento). *Nota: Entre los ejemplos de indicios de que un dispositivo puede haber sido alterado o sustituido, se pueden mencionar accesorios inesperados o cables conectados al dispositivo, etiquetas de seguridad faltantes o cambiadas, carcasas rotas o con un color diferente o cambios en el número de serie u otras marcas externas.*		2				
9.9.3 Capacite al personal para que detecten indicios de alteración o sustitución en los dispositivos. La capacitación debe abarcar lo siguiente: • Verificar la identidad de personas externas que dicen ser personal técnico o de mantenimiento antes de autorizarlos a acceder y modificar un dispositivo o solucionar algún problema. • No instalar, cambiar ni devolver dispositivos sin verificación. • Estar atentos a comportamientos sospechosos cerca del dispositivo (por ejemplo, personas desconocidas que intentan desconectar o abrir el dispositivo). • Informar al personal correspondiente sobre comportamientos sospechosos e indicios de alteración o sustitución de dispositivos (por ejemplo, a un gerente o encargado de seguridad).		2				
9.10 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.					5	
Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta						
10.1 Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.				4		
10.2 Implemente pistas de auditoría automatizadas para todos los componentes del sistema a fin de reconstruir los siguientes eventos:						
10.2.1 Todo acceso por parte de usuarios a los datos del titular de la tarjeta.				4		
10.2.2 Todas las acciones realizadas por personas con privilegios de raíz o administrativos				4		
10.2.3 Acceso a todas las pistas de auditoría				4		
10.2.4 Intentos de acceso lógico no válidos				4		
10.2.5 Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.				4		
10.2.6 Inicialización, detención o pausa de los registros de auditoría				4		
10.2.7 Creación y eliminación de objetos en el nivel del sistema				4		
10.3 Registre, al menos, las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:						
10.3.1 Identificación de usuarios				4		
10.3.2 Tipo de evento				4		
10.3.3 Fecha y hora				4		
10.3.4 Indicación de éxito o fallo				4		
10.3.5 Origen del evento				4		
10.3.6 Identidad o nombre de los datos, componentes del sistema o recursos afectados.				4		

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
10.4 Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos. *Nota: Un ejemplo de tecnología de sincronización es el NTP (protocolo de tiempo de red).*				4		
10.4.1 Los sistemas críticos tienen un horario uniforme y correcto.				4		
10.4.2 Los datos de tiempo están protegidos.				4		
10.4.3 Los parámetros de la hora se reciben de fuentes aceptadas por la industria.				4		
10.5 Resguarde las pistas de auditoría para evitar que se modifiquen.						
10.5.1 Limite la visualización de las pistas de auditoría a quienes lo necesiten por motivos laborales.				4		
10.5.2 Proteja los archivos de las pistas de auditoría contra modificaciones no autorizadas.				4		
10.5.3 Realice copias de seguridad de los archivos de las pistas de auditoría de manera oportuna en medios o servidores de registros centralizados que sean difíciles de modificar.				4		
10.5.4 Elabore registros para tecnologías externas en un dispositivo de medios o un servidor de registros interno, seguro y centralizado.				4		
10.5.5 Utilice el software de supervisión de integridad de archivos o de detección de cambios en registros para asegurarse de que los datos de los registros existentes no se puedan cambiar sin que se generen alertas (aunque el hecho de agregar nuevos datos no deba generar una alerta).				4		
10.6 Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas. *Nota: Para cumplir con este requisito, se pueden usar herramientas de recolección, análisis y alerta de registros.*						
10.6.1 Revise las siguientes opciones, al menos, una vez al día: • Todos los eventos de seguridad. • Registros de todos los componentes del sistema que almacenan, procesan o transmiten CHD y/o SAD • Registros de todos los componentes críticos del sistema. • Registros de todos los servidores y componentes del sistema que realizan funciones de seguridad (por ejemplo, firewalls, IDS/IPS [sistemas de intrusión-detección y sistemas de intrusión-prevención], servidores de autenticación, servidores de redireccionamiento de comercio electrónico, etc.).				4		
10.6.2 Revise los registros de todos los demás componentes del sistema periódicamente, de conformidad con la política y la estrategia de gestión de riesgos de la organización y según lo especificado en la evaluación anual de riesgos de la organización.				4		
10.6.3 Realice un seguimiento de las excepciones y anomalías detectadas en el proceso de revisión.				4		
10.7 Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses (por ejemplo, en línea, archivados o recuperables para la realización de copias de seguridad).				4		

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
10.8 Requisitos adicionales solo para los proveedores de servicios: Implementar un proceso para la detección oportuna y la presentación de informes de fallas de los sistemas críticos de control de seguridad, incluido pero no limitado a la falla de: • Firewalls • IDS/IPS • FIM • Antivirus • Controles de acceso físicos • Controles de acceso lógico • Mecanismos de registro de auditoría • Controles de segmentación (si se utilizan) *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*				4		
10.8.1 Requisitos adicionales solo para los proveedores de servicios: Responder a las fallas de los controles de seguridad críticos en el momento oportuno. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes: • Restaurar las funciones de seguridad • Identificar y documentar la duración (fecha y hora de inicio a fin) de la falla de seguridad • Identificar y documentar las causas de la falla, incluida la causa raíz, y documentar la remediación requerida para abordar la causa raíz • Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad • Realizar una evaluación de riesgos para determinar si se requieren más acciones como resultado de la falla de seguridad • Implementar controles para prevenir que se vuelva a producir la causa de la falla • Reanudar la supervisión de los controles de seguridad *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*				4		
10.9 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.				4		
Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.						
11.1 Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados. *Nota: Los métodos que se pueden utilizar en este proceso incluyen, entre otros, análisis de redes inalámbricas, inspecciones lógicas/físicas de los componentes y de la infraestructura del sistema, NAC (control de acceso a la red) o IDS/IPS (sistemas de intrusión-detección y sistemas de intrusión-prevención) inalámbricos. Independientemente de los métodos utilizados, deben ser suficientes para detectar e identificar tanto los dispositivos no autorizados como los autorizados.*				4		
11.1.1 Lleve un inventario de los puntos de acceso inalámbricos autorizados que incluyan una justificación comercial documentada.				4		
11.1.2 Implemente procedimientos de respuesta a incidentes en caso de que se detecten puntos de acceso inalámbricos no autorizados.		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
11.2 Realice análisis internos y externos de las vulnerabilidades de la red, al menos, trimestralmente y después de cada cambio significativo en la red (como por ejemplo, la instalación de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos). *Nota: Se pueden combinar varios informes de análisis para el proceso de análisis trimestral a fin de demostrar que se analizaron todos los sistemas y que se abordaron todas las vulnerabilidades. Es posible que se solicite documentación adicional para verificar que las vulnerabilidades no resueltas estén en proceso de resolverse.* *Para el cumplimiento inicial de las PCI DSS, no es necesario tener cuatro análisis trimestrales aprobados si el asesor verifica que 1) el resultado del último análisis fue aprobado, 2) la entidad ha documentado las políticas y los procedimientos que disponen la realización de análisis trimestrales y 3) las vulnerabilidades detectadas en los resultados del análisis se han corregido tal como se muestra en el nuevo análisis. En los años posteriores a la revisión inicial de las PCI DSS, debe haber cuatro análisis trimestrales aprobados.*		2				
11.2.1 Realice análisis interno de vulnerabilidades trimestralmente. Aborde las vulnerabilidades y realice redigitalizaciones para verificar que todas las vulnerabilidades de "alto riesgo" se resuelven de acuerdo con la clasificación de la vulnerabilidad de la entidad (según el Requisito 6.1). Los análisis deben estar a cargo de personal calificado.		2				
11.2.2 Los análisis trimestrales de vulnerabilidades externas deben estar a cargo de un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC (PCI Security Standards Council). Vuelva a realizar los análisis cuantas veces sea necesario hasta que todos los análisis estén aprobados. *Nota: Los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor aprobado de análisis (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC). Consulte la Guía del programa de ASV (proveedor aprobado de escaneo) publicada en el sitio web del PCI SSC para obtener información sobre las responsabilidades de análisis del cliente, sobre la preparación del análisis, etc.*		2				
11.2.3 Lleve a cabo análisis internos y externos, y repítalos, según sea necesario, después de realizar un cambio significativo. Los análisis deben estar a cargo de personal calificado.		2				
11.3 Implemente una metodología para las pruebas de penetración que incluya lo siguiente: • Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800-115). • Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos. • Incluya pruebas del entorno interno y externo de la red. • Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance. • Defina las pruebas de penetración de la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el requisito 6.5 • Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos. • Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses. • Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección.		2				
11.3.1 Lleve a cabo pruebas de penetración externas, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno).		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
11.3.2 Lleve a cabo pruebas de penetración internas, al menos, una vez al año y después de implementar una actualización o modificación significativa en las infraestructuras o aplicaciones (como por ejemplo, actualizar el sistema operativo, agregar una subred o un servidor web al entorno).		2				
11.3.3 Las vulnerabilidades de seguridad detectadas en las pruebas de penetración se corrigen, y las pruebas se repiten para verificar las correcciones.		2				
11.3.4 Si se usa la segmentación para aislar el CDE (entorno de datos del titular de la tarjeta) de otras redes, realice pruebas de penetración, al menos, una vez al año y después de implementar cambios en los métodos o controles de segmentación para verificar que los métodos de segmentación sean operativos y efectivos, y que aíslen todos los sistemas fuera de alcance de los sistemas en el CDE.		2				
11.3.4.1 Requisitos adicionales solo para los proveedores de servicios: Si se utiliza la segmentación, confirme el alcance de la PCI DSS al realizar pruebas de penetración en los controles de segmentación al menos cada seis meses, y después de cualquier cambio a los controles/métodos de segmentación. *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*		2				
11.4 Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. Monitoree todo el tráfico presente en el perímetro del entorno de datos del titular de la tarjeta y en los puntos críticos del entorno de datos del titular de la tarjeta, y alerte al personal ante la sospecha de riesgos. Mantenga actualizados todos los motores de intrusión-detección y de prevención, las bases y firmas.		2				
11.5 Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de integridad de archivos) para alertar al personal sobre modificaciones (incluyendo cambios, adiciones y eliminaciones) no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y configure el software para realizar comparaciones de archivos críticos, al menos, una vez por semana. *Nota: A los fines de la detección de cambios, generalmente, los archivos críticos son aquellos que no se modifican con regularidad, pero cuya modificación podría implicar un riesgo o peligro para el sistema. Generalmente, los mecanismos de detección de cambios, como los productos de supervisión de integridad de archivos, vienen preconfigurados con archivos críticos para el sistema operativo relacionado. La entidad (es decir el comerciante o el proveedor de servicios) debe evaluar y definir otros archivos críticos, tales como los archivos para aplicaciones personalizadas.*				4		
11.5.1 Implemente un proceso para responder a las alertas que genera la solución de detección de cambios.				4		
11.6 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.				4		
Requisito 12: Mantener una política que aborde la seguridad de la información para todo el personal						
12.1 Establezca, publique, mantenga y distribuya una política de seguridad.						6
12.1.1 Revise la política de seguridad, al menos, una vez al año y actualícela cuando se realicen cambios en el entorno.						6

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
12.2 Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente: • Se realiza, al menos, una vez al año y después de implementar cambios significativos en el entorno (por ejemplo, adquisiciones, fusiones o reubicaciones, etc.) • Identifica activos críticos, amenazas y vulnerabilidades. • Los resultados en un análisis formal y documentado de riesgo. Los ejemplos de metodologías de evaluación de riesgos incluyen, entre otros, OCTAVE, ISO 27005 y NIST SP 800-30.	1					
12.3 Desarrolle políticas de uso para las tecnologías críticas y defina cómo usarlas correctamente. *Nota: Entre los ejemplos de tecnologías críticas, se incluyen las tecnologías inalámbricas y de acceso remoto, las computadoras portátiles, las tabletas, los dispositivos electrónicos extraíbles, el uso del correo electrónico y de Internet.* Asegúrese de que estas políticas de uso requieran lo siguiente:						6
12.3.1 Aprobación explícita de las partes autorizadas						6
12.3.2 Autenticación para el uso de la tecnología						6
12.3.3 Lista de todos los dispositivos y el personal que tenga acceso						6
12.3.4 Método para determinar, con exactitud y rapidez, el propietario, la información de contacto y el objetivo (por ejemplo, etiquetado, codificación o inventario de dispositivos).						6
12.3.5 Usos aceptables de la tecnología						6
12.3.6 Ubicaciones aceptables de las tecnologías en la red						6
12.3.7 Lista de productos aprobados por la empresa						6
12.3.8 Desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad						6
12.3.9 Activación de las tecnologías de acceso remoto para proveedores y socios de negocio sólo cuando sea necesario, con desactivación inmediata después de su uso						6
12.3.10 En el caso del personal que tiene acceso a los datos del titular de la tarjeta mediante tecnologías de acceso remoto, prohíba copiar, mover y almacenar los datos del titular de la tarjeta en unidades de disco locales y en dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente para una necesidad comercial definida. Si existe una necesidad comercial autorizada, las políticas de uso deben disponer la protección de los datos de conformidad con los requisitos correspondientes de las PCI DSS.						6
12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan, claramente, las responsabilidades de seguridad de la información de todo el personal.						6
12.4.1 Requisitos adicionales solo para los proveedores de servicios: La gerencia ejecutiva deberá establecer la responsabilidad de la protección de los datos del titular de la tarjeta y un programa de cumplimiento de la PCI DSS para incluir: • Responsabilidad general de mantener el cumplimiento de la PCI DSS • Definir un estatuto para el programa de cumplimiento de la PCI DSS y la comunicación a la gerencia ejecutiva *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*						6

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
12.5 Asigne a una persona o a un equipo las siguientes responsabilidades de administración de seguridad de la información:						6
12.5.1 Establezca, documente y distribuya las políticas y los procedimientos de seguridad.						6
12.5.2 Monitoree y analice las alertas y la información de seguridad y comuníquelas al personal correspondiente.						6
12.5.3 Establezca, documente y distribuya los procedimientos de escalamiento y respuesta ante incidentes de seguridad para garantizar un manejo oportuno y efectivo de todas las situaciones.		2				
12.5.4 Administre las cuentas de usuario, incluso las incorporaciones, eliminaciones y modificaciones.						6
12.5.5 Monitoree y controle todo acceso a los datos.						6
12.6 Implemente un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de la importancia de la seguridad de los datos del titular de la tarjeta.						6
12.6.1 Capacite al personal inmediatamente después de contratarlo y, al menos, una vez al año. Nota: Los métodos pueden variar según el rol del personal y del nivel de acceso a los datos del titular de la tarjeta.						6
12.6.2 Exija al personal que realice, al menos, una vez al año, una declaración de que leyeron y entendieron la política y los procedimientos de seguridad de la empresa.						6
12.7 Examine al personal potencial antes de contratarlo a fin de minimizar el riesgo de ataques desde fuentes internas. (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias). *Nota: En el caso de los posibles candidatos para ser contratados, como cajeros de un comercio, que solo tienen acceso a un número de tarjeta a la vez al realizar una transacción, este requisito es solo una recomendación.*						6
12.8 Mantenga e implemente políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta de la siguiente manera:		2				
12.8.1 Mantener una lista de proveedores de servicios, incluida una descripción del servicio prestado.		2				
12.8.2 Mantenga un acuerdo por escrito en el que los proveedores de servicios aceptan responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. *Nota: La redacción exacta del reconocimiento dependerá del acuerdo existente entre las dos partes, los detalles del servicio prestado y las responsabilidades asignadas a cada parte. No es necesario que el reconocimiento incluya el texto exacto de este requisito.*		2				
12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios, que incluya una auditoría adecuada previa al compromiso.		2				
12.8.4 Mantenga un programa para monitorear el estado de cumplimiento de las PCI DSS por parte del proveedor de servicios.		2				
12.8.5 Conserve información sobre cuáles son los requisitos de las PCI DSS que administra cada proveedor de servicios y cuáles administra la entidad.		2				

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
12.9 Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios aceptan, por escrito y ante los clientes, responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente. *Nota: La redacción exacta del reconocimiento dependerá del acuerdo existente entre las dos partes, los detalles del servicio prestado y las responsabilidades asignadas a cada parte. No es necesario que el reconocimiento incluya el texto exacto de este requisito.*		2				
12.10 Implemente un plan de respuesta ante incidentes. Prepárese para responder de inmediato ante un fallo en el sistema.						
12.10.1 Desarrolle el plan de respuesta ante incidentes que se implementará en caso de que ocurra una falla del sistema. Asegúrese de que el plan aborde, como mínimo, lo siguiente: • Roles, responsabilidades y estrategias de comunicación y contacto en caso de un riesgo que incluya, como mínimo, la notificación de las marcas de pago. • Procedimientos específicos de respuesta a incidentes. • Procedimientos de recuperación y continuidad comercial. • Procesos de copia de seguridad de datos. • Análisis de los requisitos legales para el informe de riesgos. • Cobertura y respuestas de todos los componentes críticos del sistema. • Referencia o inclusión de procedimientos de respuesta ante incidentes de las marcas de pago.		2				
12.10.2 Revise y pruebe el plan, incluidos todos los elementos enumerados en el Requisito 12.10.1, al menos anualmente.		2				
12.10.3 Designe a personal específico para que esté disponible las 24 horas al día, los 7 días de la semana para responder a las alertas.		2				
12.10.4 Capacite adecuadamente al personal sobre las responsabilidades de respuesta ante fallas de seguridad.		2				
12.10.5 Incluya alertas de los sistemas de supervisión de seguridad, que incluye, entre otros, sistemas de intrusión-detección y de intrusión-prevención, firewalls y sistemas de supervisión de integridad de archivos.		2				
12.10.6 Elabore un proceso para modificar y desarrollar el plan de respuesta ante incidentes según las lecciones aprendidas e incorporar los desarrollos de la industria.		2				
12.11 Requisitos adicionales solo para los proveedores de servicios: Realizar revisiones al menos trimestralmente para confirmar que el personal sigue las políticas de seguridad y los procedimientos operativos. Las revisiones deben cubrir los siguientes procesos: • Revisiones del registro diario • Revisiones del conjunto de reglas de firewall • La aplicación de las normas de configuración a los nuevos sistemas • Respuesta a las alertas de seguridad • Procesos de gestión del cambio *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*						6

Requisitos de las PCI DSS v3.2	Hitos					
	1	2	3	4	5	6
12.11.1 Requisitos adicionales solo para los proveedores de servicios: Mantener la documentación del proceso de revisión trimestral para incluir: • Documentar los resultados de las revisiones • Revisar y cerrar los resultados por parte del personal asignado para asumir la responsabilidad del programa de cumplimiento de las PCI DSS *Nota: Este requisito se considerará la mejor práctica hasta el 31 de enero de 2018 y, a partir de ese momento, se convertirá en requisito.*						6
Anexo A1: Requisitos de la PCI DSS adicionales para proveedores de hosting compartido						
A.1 Proteger el entorno y los datos alojados de cada entidad (es decir comerciante, proveedor de servicios u otra entidad), según los puntos A.1.1 a A.1.4: Un proveedor de hosting debe cumplir con estos requisitos, así como también con las demás secciones correspondientes de PCI DSS. *Nota: Aunque posiblemente el proveedor de hosting cumpla con estos requisitos, no se garantiza el cumplimiento de la entidad que utiliza al proveedor de hosting. Cada entidad debe cumplir con las PCI DSS y validar el cumplimiento, según corresponda.*			3			
A.1.1 Asegúrese de que cada entidad solo implemente procesos que tengan acceso al entorno de datos del titular de la tarjeta de la entidad.			3			
A.1.2 Limite el acceso y los privilegios de cada entidad solo al entorno de sus propios datos del titular de la tarjeta.			3			
A.1.3 Asegúrese de que los registros y las pistas de auditoría estén habilitados y sean exclusivos para el entorno de datos del titular de la tarjeta de cada entidad y que cumplan con el Requisito 10 de las PCI DSS.			3			
A1.4 Habilite los procesos para que se realice una investigación forense oportuna en caso de que un comerciante o proveedor de servicios alojado corra riesgos.			3			
Anexo A2: Requisitos de la PCI DSS adicionales para las entidades que utilizan SSL/TLS temprana *Nota: Este Anexo se aplica a las entidades que utilizan SSL/TLS temprana como un control de seguridad para proteger el CDE y/o CHD*						
A2.1 Donde las terminales POS POI (y los puntos de terminación de SSL/TLS a los que se conectan) utilizan SSL y/o TLS temprana, la entidad debe • Confirmar que los dispositivos no son susceptibles a los ataques conocidos para aquellos protocolos. O: • Tener un Plan de migración y de mitigación de riesgo formal implementado.		2				
A2.2 Las entidades con las implementaciones existentes (excepto según lo permitido en A2.1) que utilizan SSL y/o TLS temprana deben tener un Plan de Migración y de mitigación del riesgo implementados.		2				
A2.3 Requisitos adicionales solo para los proveedores de servicios: Todos los proveedores de servicios deben ofrecer una oferta de servicios segura al 30 de junio de 2016. *Nota: Con anterioridad al 30 de junio de 2016, el proveedor de servicios debe tener una opción de protocolo seguro incluida en su oferta de servicios, o tener un Plan de migración y mitigación de riesgos documentado (según A2.2) que incluya una fecha límite para la provisión de una opción de protocolo seguro no más tarde del 30 de junio de 2016. Después de esta fecha, todos los proveedores de servicios deben ofrecer una opción de protocolo seguro para su servicio.*		2				