Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI)

Procedimientos de Auditoría de Seguridad

Versión 1.1

Publicada: Septiembre 2006

Contenido

Introducción ... 3
Información sobre Aplicabilidad de las Normas de Seguridad de Datos la Industria de Tarjetas Bancarias ... 4
Alcance de la Evaluación del Cumplimiento con los Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago ... 5
- Medios Inalámbricos ... 6
- Subcontratación ... 6
- Muestreo ... 6
- Controles Compensatorios ... 7

Instrucciones y Contenido para Reportes de Cumplimiento ... 7
- Revaluación de Puntos Abiertos ... 9

Desarrollar y Mantener Una Red Segura ... 9
- Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los tarjetahabientes ... 9
- Requisito 2: No usar contraseñas de sistemas y otros parámetros de seguridad provistos por suplidores. ... 14

Proteger los Datos de los Tarjetahabientes ... 18
- Requisito 3: Proteger los Datos Almacenados ... 18
- Requisito 4: Encriptar la transmisión de datos de tarjetahabientes a través de redes públicas abiertas ... 26

Mantener un Programa de Manejo de Vulnerabilidad ... 29
- Requisito 5: Usar y actualizar regularmente el software o programas antivirus ... 29
- Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras ... 30

Implementar Medidas Sólidas de Control de Acceso ... 36
- Requisito 7: Restringir el acceso a los datos de los tarjetahabientes tomando como base la necesidad del funcionario de conocer la información ... 36
- Requisito 8: Asignar una ID única a cada persona que tenga acceso a los computadores. ... 37
- Requisito 9: Restringir el acceso físico a los datos de los tarjetahabientes. ... 43

Monitorear y Probar Regularmente las Redes ... 47
- Requisito 10: Rastrear y monitorear todo el acceso a los recursos de la red y datos de los tarjetahabientes ... ??
- Requisito 11: Probar regularmente los sistemas y procesos de seguridad. ... 51

Mantener una Política de Seguridad de Información ... 54
- Requisito 12: Mantener una política que contemple la seguridad de la información para los empleados y contratistas. ... 54

Apéndice A: Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para los Proveedores de Servicios de Hospedaje en Redes (con Procedimientos para Pruebas) ... 61
- Requisito A.1: Protección del ambiente de datos de los tarjetahabientes por parte del proveedor de servicios de hospedaje ... 61

Apéndice B – Controles Compensatorios ... 65
- Controles Compensatorios – Generales ... 65
- Controles Compensatorios para el Requisito 3.4 ... 65

Apéndice C: Hoja de Trabajo de Controles Compensatorios/Ejemplo ... 66

Introducción

Los Procedimientos de Auditoría de Seguridad de la Industria de Tarjetas de Pago (PCI) están diseñados para ser utilizados por los evaluadores que realizan las revisiones in situ de los comercios y proveedores de servicio a quienes se requiere validar el cumplimiento con los Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago. Los requisitos y procedimientos de auditoría presentados en este documento están basados en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS).

Este documento contiene lo siguiente:

- **Introducción**
- **Información sobre la Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago**
- **Alcance de la Evaluación para el Cumplimiento de los Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago**
- **Instrucciones y Contenido del *Reporte de Cumplimiento***
- **Revalidación de Puntos Abiertos**
- **Procedimientos de Auditoría de Seguridad**

APÉNDICES

- **Apéndice A: Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para Proveedores de Servicio de Hospedaje en Redes (con Procedimientos para Pruebas)**
- **Apéndice B: Controles Compensatorios**
- **Apéndice C: Hoja de Trabajo de Controles Compensatorios/Ejemplo**

Información sobre la Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago

La tabla siguiente ilustra los elementos de datos confidenciales de los tarjetahabientes y de autenticación que normalmente se usan; si se permite o se prohíbe **guardar** cada elemento de datos y **si se requiere proteger cada elemento de datos**. Esta tabla no es exhaustiva, pero se presenta para ilustrar los distintos tipos de requisitos que se aplican a cada elemento de datos.

	Elemento de Datos	Se permite guardar	Protección requerida	PCI DSS REQ. 3.4
Datos de los Tarjetahabientes	Número de Cuenta Primario (PAN)*	SÍ	SÍ	SÍ
	Nombre del Tarjetahabiente*	SÍ	SÍ*	NO
	Código de Servicio*	SÍ	SÍ*	NO
	Fecha de Vencimiento*	SÍ	SÍ*	NO
Datos Confidenciales de Autenticación**	Contenido de la banda magnética	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / Bloque de PIN	NO	N/A	N/A

** Se requiere proteger estos elementos de datos si se guardan junto con el Número de Cuenta Primario (PAN). Esta protección debe cumplir con los requisitos establecidos en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) para la protección general del ambiente de tarjetahabientes. Además, otras leyes (por ejemplo, las relacionadas con la protección de los datos personales de los consumidores, la privacidad, el robo de identidad y la seguridad de datos) pueden requerir protecciones específicas para estos datos o la divulgación apropiada de las prácticas de privacidad de la empresa si se recopilan datos personales de los consumidores en el curso del negocio. Sin embargo, las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) no se aplican si no se guardan, procesan o transmiten números de cuenta primarios (PAN).*

*** Los datos de autenticación confidenciales, que tienen alta sensitividad, no deberán guardarse después de la autorización (aunque estén encriptados).*

Alcance de la Evaluación del Cumplimiento con los Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago

Los Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago se aplican a todos los "componentes de sistemas". Los componentes de sistemas se definen como cualquier componente de red, servidor o aplicación incluido o conectado al ambiente de datos de los tarjetahabientes. El ambiente de datos de los tarjetahabientes es la parte de la red que posee los datos de los tarjetahabientes o los datos confidenciales de autenticación. Los componentes de red incluyen, sin limitación, cortafuegos, switches, ruteadores, puntos de acceso inalámbrico, aparatos conectados a la red y otros aparatos y dispositivos de seguridad. Los tipos de servidores incluyen, sin limitación, los siguientes: Web, base de datos, autenticación, correo, proxy, Network Time Protocol (NTP) y servidores de nombre de dominio (DNS). Las aplicaciones incluyen todas las aplicaciones adquiridas comercialmente o individualmente desarrolladas, incluyendo aplicaciones internas y externas (Internet).

Una segmentación adecuada de la red, que aísla los sistemas que guardan, procesan o transmiten datos de los tarjetahabientes de aquellos que no realizan estas funciones, podría reducir el alcance del ambiente de datos de los tarjetahabientes. El evaluador debe verificar que la segmentación es la adecuada para reducir el alcance de la auditoría.

Un proveedor de servicio o comercio puede utilizar a un tercero para administrar componentes como ruteadores, cortafuegos, bases de datos, seguridad física y/o servidores. Si es así, es posible que haya un impacto en la seguridad del ambiente de datos de los tarjetahabientes. Los servicios relevantes del tercero deben escrutinizarse en 1) cada auditoría basada en las normas PCI que se realice de los clientes del tercero; o 2) la auditoría de las normas PCI del propio tercero.

En el caso de los proveedores de servicio que estén bajo el requisito de pasar una evaluación anual en sus propios locales, la validación del cumplimiento se deberá realizar en todos los componentes de sistemas en los cuales se procesen, guarden o transmitan datos de los tarjetahabientes, a menos que se especifique otra cosa.

En el caso de los comercios que estén bajo la obligación de pasar una evaluación anual en sus propios locales, la validación del cumplimiento se concentra en cualquier componente de sistema relacionado con la autorización y la liquidación donde se procesan, guardan o transmiten datos de los tarjetahabientes, incluyendo los siguientes:

- Todas las conexiones externas a la red del comercio (por ejemplo, acceso remoto de los empleados, compañía de tarjetas de pago, acceso de terceros para fines de procesamiento y mantenimiento)
- Todas las conexiones al y del ambiente de autorización y liquidación (por ejemplo, conexiones para acceso de empleados o para dispositivos como cortafuegos y ruteadores)
- Cualquier repositorio de datos fuera del ambiente de autorización y liquidación donde se guarden más de 500,000 números de cuenta. Nota: Aunque se excluyan de la auditoría algunos repositorios o sistemas de datos, el comercio sigue siendo responsable de asegurar que todos los sistemas que guarden, procesen o transmitan datos de los tarjetahabientes cumplan con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.

- El ambiente de punto de venta (POS)– el lugar donde se acepta una transacción en un establecimiento (es decir, una tienda minorista, restaurante, hotel, estación de gasolina u otra ubicación que tenga un punto de venta)
- Si no hay acceso externo al local de comercio (por Internet, inalámbrico, red privada virtual o VPN, marcado telefónico, ancho de banda o máquinas públicamente accesibles como quioscos), se puede excluir el ambiente de punto de venta

Medios Inalámbricos

Si se usa la tecnología inalámbrica para guardar, procesar o transmitir datos de los tarjetahabientes (por ejemplo, transacciones de punto de venta, “line-busting”, etc.), o hay una red de acceso local (LAN) inalámbrica conectada al ambiente de datos de los tarjetahabientes o a una parte del mismo (es decir, que no esté claramente separada por un cortafuego), se aplican y deben implementarse los Requisitos y Procedimientos de Prueba para ambientes inalámbricos también. La seguridad en los medios inalámbricos aún no ha madurado lo suficiente, pero estos requisitos especifican la implementación de funciones de seguridad inalámbrica básicas para proporcionar una protección mínima. Puesto que aún no se puede garantizar la seguridad de las tecnologías inalámbricas, recomendamos que antes de implementarlas la compañía debe evaluar cuidadosamente la necesidad de contar con esta tecnología tomando en consideración el riesgo. Considere implementar la tecnología inalámbrica solamente para las transmisiones de datos no confidenciales o esperar a que la tecnología sea más segura.

Subcontratación

En el caso de las entidades que subcontratan funciones o servicios de almacenaje, procesamiento o transmisión de datos de los tarjetahabientes a terceros, el *Reporte de Cumplimiento* debe documentar el papel de cada proveedor de servicio. Además, cada proveedor de servicio es responsable de validar su propio cumplimiento con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago, independientemente de las auditorías de sus clientes. Además, los comercios y proveedores de servicio deberán requerir contractualmente a todo tercero con quien se asocien que tenga acceso a los datos de los tarjetahabientes que se adhiera a los Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Consulte el Requisito 12.8 de este documento para obtener información más detallada.

Muestreo

El evaluador puede seleccionar una muestra representativa de componentes de sistemas para probarlos. La muestra debe ser una selección representativa de todos los tipos de componentes de sistemas e incluir una variedad de sistemas operativos, funciones y aplicaciones según se apliquen al área revisada. Por ejemplo, el revisor podría elegir los servidores Sun que operan con Apache WWW, los servidores NT que operan con Oracle, los sistemas mainframe que operan con aplicaciones heredadas de procesamiento de tarjetas, los servidores de transferencia de datos que operan con HP-UX y servidores Linux que operan con MYQL, etc. Si todas las aplicaciones operan desde un mismo sistema operativo (por ejemplo, NT, Sun, etc.), la muestra deberá incluir una variedad de aplicaciones (por ejemplo, servidores de base de datos, servidores de Web y servidores de transferencia de datos, etc.).

Al seleccionar muestras de las tiendas de los comercios o en el caso de los comercios que son franquicias, los evaluadores deberán considerar lo siguiente:

- Si los procesos estándar requeridos por las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago que cada tienda debe seguir están implementados la muestra puede ser menor de lo que sería necesario si no hubiese procesos estándar, a fin de proporcionar una certeza razonable de que cada tienda está configurada de acuerdo con el proceso estándar.
- Si hay más de un tipo de proceso estándar implementado (por ejemplo, para diferentes tipos de tiendas), entonces la muestra debe ser lo suficientemente grande como para incluir las tiendas aseguradas con cada tipo de proceso.
- Si no hay procesos estándar de Normas de Seguridad de Datos de la Industria de Tarjetas de Pago implementados y cada tienda es responsable por sus propios procesos, entonces el tamaño de la muestra debe ser lo suficientemente grande como para tener la certeza de que cada tienda entiende e implementa en forma apropiada los requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.

Controles Compensatorios

El evaluador deberá documentar los controles compensatorios e incluirlos con el Reporte de Cumplimiento que presente, según se ilustra en el Apéndice C – Hoja de Trabajo de Controles Compensatorios/Ejemplo.

Vea el Glosario de Términos, Abreviaturas y Acrónimos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para obtener la definición de “controles compensatorios”.

Instrucciones y Contenido del Reporte de Cumplimiento

Los evaluadores utilizarán este documento como modelo para crear el *Reporte de Cumplimiento*. La entidad auditada deberá seguir los requisitos de reporte de cada compañía de tarjetas de pago para asegurar que cada compañía reconozca el estado de cumplimiento de la entidad. Comuníquese con cada compañía de tarjetas de pago para determinar los requisitos e instrucciones de reporte de cada compañía. Todos los evaluadores deberán seguir las instrucciones relacionadas con el contenido y formato del reporte al completar un *Reporte de Cumplimiento*:

1. Información de Contacto y Fecha del Reporte

- Incluya la información de contacto del comercio o proveedor de servicio y del evaluador.
- Fecha del reporte.

2. Resumen Ejecutivo

Incluir lo siguiente:

- Descripción del negocio
- Lista de proveedores de servicio y otras entidades con quien la compañía comparte los datos de los tarjetahabientes.

- Lista de relaciones con procesadores.
- Describa si la entidad está directamente conectada a una compañía de tarjetas de pago.
- En el caso de los comercios, los productos de punto de venta que se utilizan.
- Cualquier entidad en propiedad absoluta que requiera cumplir con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.
- Cualquier entidad internacional que requiera cumplir con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.
- Cualquier red de acceso local (LAN) inalámbrica o terminal de punto de venta inalámbrico conectado al ambiente de datos de los tarjetahabientes.

3. Descripción del Alcance del Trabajo y Enfoque Adoptado

- Versión del documento de Procedimientos de Auditoría de Seguridad utilizado para realizar la evaluación.
- Plazo de la evaluación.
- Ambiente en el cual se concentró la evaluación (por ejemplo, puntos de acceso a Internet del cliente, red corporativa interna, puntos de procesamiento de la compañía de tarjetas de pago, etc.).
- Cualquier área excluida de la revisión.
- Breve descripción o diagrama de alto nivel de la topología y los controles de la red.
- Lista de las personas consultadas.
- Lista de documentos revisados.
- Lista de hardware y software crítico en uso (por ejemplo, base de datos o encriptación).
- En el caso de las revisiones de Proveedores de Servicio Administrados (Managed Service Provider o MSP), delinear claramente cuáles requisitos de este documento se aplican a los mismos (y se incluyen en la revisión) y cuáles no se incluyen en la revisión y son responsabilidad de los clientes de dichos proveedores, a incluir en sus propias revisiones. Incluya información sobre cuáles direcciones de Internet (IP) se escanean como parte de los escanes de vulnerabilidad trimestrales de los proveedores de servicio administrados, y cuáles direcciones de Internet son responsabilidad de los clientes de dichos proveedores a incluir en sus propios escanes trimestrales.

4. Resultados de Escán Trimestral

- Resumir brevemente los resultados de los últimos 4 escanes trimestrales en los comentarios del Requisito 11.2.
- El escán debe cubrir todas las direcciones de Internet (IP hacia Internet) en existencia en la entidad.

5. Hallazgos y Observaciones

- Todos los evaluadores deberán utilizar el siguiente modelo para proporcionar descripciones detalladas en el reporte y describir los hallazgos en cada requisito y subrequisito.

- Donde aplique, documentar cualquier control compensatorio considerado para concluir que se ha establecido adecuadamente un control.
- Vea el Glosario de Términos, Abreviaturas y Acrónimos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para obtener la definición de “controles compensatorios”.

Revalidación de Puntos Abiertos

Para validar el cumplimiento se requiere un reporte de controles establecidos. Si hay puntos abiertos en el reporte inicial del auditor/evaluador, el comercio o proveedor de servicio deberá corregir todos estos puntos abiertos. El auditor/ evaluador deberá revalidar que se han tomado las medidas remediales apropiadas y se han llenado todos los requisitos. Después de la revalidación el evaluador emitirá un nuevo *Reporte de Cumplimiento* verificando que el sistema cumple con todos los requisitos y lo presentará según las instrucciones (ver anteriormente).

Desarrollar y Mantener una Red Segura

Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los tarjetahabientes.

Los cortafuegos son dispositivos computarizados que controlan el tráfico de entrada y salida permitido en la red de una compañía, así como el tráfico a áreas más sensibles dentro de la red interna de la compañía. El cortafuego examina todo el tráfico de la red y bloquea las transmisiones que no cumplen con los criterios especificados.

Es necesario proteger todos los sistemas contra el acceso no autorizado desde Internet, sea para fines de comercio electrónico, acceso a Internet desde los computadores de mesa de los empleados o acceso al correo electrónico de los empleados. Con frecuencia algunas vías de conexión hacia y desde la Internet aparentemente insignificantes pueden proporcionar un acceso sin protección a sistemas clave. Los cortafuegos son un mecanismo de protección esencial para cualquier red de computadores.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
1.1 Establecer normas de configuración de cortafuegos que incluyan lo siguiente:	**1.1** Obtener e inspeccionar las normas de configuración de cortafuegos y otros documentos especificados abajo para verificar que las normas se han implementado completamente. Completar cada punto en esta sección:			
1.1.1 Un proceso formal para aprobar y probar todas las conexiones externas de la red y los cambios a la configuración de cortafuegos.	**1.1.1** Verificar que las normas de configuración de cortafuegos incluyen un proceso formal para todos los cambios en los cortafuegos, incluyendo pruebas y la aprobación de la administración para todos los cambios a las conexiones externas y configuración de cortafuegos.			
1.1.2 Un diagrama actualizado de la red con todas las conexiones que acceden a los datos de los tarjetahabientes, incluyendo cualquier red inalámbrica.	**1.1.2.a** Verificar que existe un diagrama actualizado de la red y verificar que el mismo documenta todas las conexiones a los datos de los tarjetahabientes, incluyendo cualquier red inalámbrica.			
	1.1.2.b Verificar que el diagrama se mantiene al día.			
1.1.3 Requisitos para tener un cortafuego en cada conexión a Internet y entre cualquier zona desmilitarizada (DMZ) y la zona de la red interna.	**1.1.3** Verificar que las normas de configuración de cortafuegos incluyen requisitos para tener un cortafuego en cada conexión de Internet y entre cualquier DMZ y la Intranet. Verificar que el diagrama actual de la red es congruente con las normas de configuración de cortafuegos.			
1.1.4 Descripción de grupos, roles y responsabilidades para una administración lógica de los componentes de la red.	**1.1.4** Verificar que las normas de configuración de cortafuegos incluyen una descripción de grupos, papeles y responsabilidades de administración lógica de los componentes de la red.			
1.1.5 Lista documentada de servicios y puertos necesarios para las actividades del negocio.	**1.1.5** Verificar que las normas de configuración de cortafuegos incluyen una lista documentada de los servicios y puertos necesarios para las actividades del negocio.			
1.1.6 Justificación y documentación de cualquier protocolo disponible aparte de Hypertext Transfer Protocol (HTTP) y Secure Sockets Layer (SSL,) Secure Shell (SSH,) y Virtual	**1.1.6** Verificar que las normas de configuración de cortafuegos incluyen justificación y documentación de cualquier protocolo disponible además de HTTP y SSL, SSH y VPN.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
Private Network (VPN).				
1.1.7 Justificación y documentación de cualquier protocolo riesgoso permitido (por ejemplo, File Transfer Protocol o FTP), que incluya la razón para usar el protocolo y las funciones de seguridad implementadas.	**1.1.7.a** Verificar que las normas de configuración de cortafuegos incluyen justificación y documentación de cualquier protocolo riesgoso permitido (por ejemplo, FTP), que incluye la razón para el uso del protocolo y las funciones de seguridad implementadas.			
	1.1.7.b Examinar la documentación y parámetros programados de cada servicio que esté en uso para obtener evidencia de que el servicio es necesario y seguro.			
1.1.8 Revisión trimestral de los conjuntos de reglas de cortafuegos y ruteadores.	**1.1.8.a** Verificar que las normas de configuración de cortafuegos requieren una revisión trimestral de los conjuntos de reglas de cortafuegos y ruteadores.			
	1.1.8.b Verificar que los conjuntos de reglas se revisan cada trimestre.			
1.1.9 Normas de configuración de ruteadores	**1.1.9** Verificar que existen normas de configuración de cortafuegos tanto para los cortafuegos como para los ruteadores.			
1.2 Desarrollar una configuración de cortafuegos que bloquee todo el tráfico de redes y hosts “no confiables”, excepto protocolos necesarios para el ambiente de datos de los tarjetahabientes.	**1.2** Elegir una muestra de cortafuegos/ruteadores 1) entre Internet y el DMZ y 2) entre el DMZ y la red interna. La muestra debe incluir el ruteador choke en Internet, el ruteador de DMZ y el cortafuego, el segmento de tarjetahabientes del DMZ, el ruteador perimétrico y el segmento de tarjetahabientes de la red interna. Examinar las configuraciones de cortafuegos y ruteadores para verificar que el tráfico de entrada y salida está limitado a solamente protocolos que sean necesarios para el ambiente de datos de los tarjetahabientes.			
1.3 Desarrollar una configuración de cortafuegos que restrinja las conexiones entre los servidores públicamente accesibles y cualquier componente de sistemas que guarde	**1.3** Examinar las configuraciones de cortafuegos/ruteadores para verificar que las conexiones están restringidas entre los servidores públicamente accesibles y los componentes que guardan datos de los tarjetahabientes, de la manera			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
datos de los tarjetahabientes, incluyendo cualquier conexión de redes inalámbricas. Esta configuración de cortafuegos debe incluir:	siguiente:			
1.3.1 Restringir el tráfico entrante de Internet a las direcciones IP (Internet Protocol) dentro del DMZ (filtros de ingreso).	**1.3.1** Verificar que el tráfico de entrada de Internet está limitado a direcciones de Internet (IP) dentro del DMZ.			
1.3.2. No permitir que las direcciones internas pasen de Internet al DMZ	**1.3.2** Verificar que las direcciones internas de Internet no pueden pasar de Internet al DMZ.			
1.3.3 Implementar la inspección completa, también conocida como filtrado dinámico de paquetes (es decir, solamente se permite. entrada a la red a través de las conexiones “establecidas”).	**1.3.3** Verificar que el cortafuego realiza una inspección completa (filtro de paquete dinámico). (Solamente debe permitirse la entrada a través de conexiones establecidas y solamente si las mismas están asociadas con una sesión previamente establecida (ejecutar NMAP en todos los Puertos TCP con el conjunto de bits “syn reset” o ”syn ack”– una respuesta significa que se permite la entrada a paquetes aunque no formen parte de una sesión previamente establecida).			
1.3.4 Colocar la base de datos en una zona interna de la red, segregada del DMZ.	**1.3.4** Verificar que la base de datos está en una zona interna de la red, segregada del DMZ.			
1.3.5 Restringir el tráfico entrante y saliente a aquel que sea necesario para el ambiente de datos de tarjetahabientes.	**1.3.5** Verificar que el tráfico entrante y saliente está limitado al que es necesario para el ambiente de los tarjetahabientes y que las restricciones están documentadas.			
1.3.6 Asegurar y sincronizar los archivos de configuración de ruteador. (Por ejemplo, los archivos de configuración (para el funcionamiento normal de los ruteadores) y los archivos de configuración de inicio de operaciones (cuando se hace un *re-*	**1.3.6** Verificar que los archivos de configuración del ruteador son seguros y están sincronizados (por ejemplo, que los archivos de configuración que se utilizan para la operación normal de los ruteadores, y los archivos de configuración de inicio de operaciones que se utilizan cuando se hace un re-booting de las máquinas, tienen las mismas configuraciones seguras).			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
booting de las máquinas), deben tener la misma configuración segura).				
1.3.7 Rechazar todo el tráfico entrante y saliente de Internet que no esté específicamente permitido.	**1.3.7** Verificar que todo el tráfico de otra índole de entrada y de salida no contemplado en el 1.2 y 1.3 anteriormente se rechace específicamente.			
1.3.8 Instalar cortafuegos perimétricos entre cualquier red inalámbrica y el ambiente de datos de los tarjetahabientes y configurar estos cortafuegos para rechazar cualquier tráfico del ambiente inalámbrico o controlar (si dicho tráfico es necesario para los fines del negocio) todo el tráfico desde el ambiente inalámbrico.	**1.3.8** Verificar que hay cortafuegos perimétricos instalados entre cualquier red inalámbrica y sistema que guarde datos de los tarjetahabientes, y que estos cortafuegos rechazan o controlan (si dicho tráfico es necesario para fines comerciales) cualquier tráfico desde el ambiente inalámbrico a los sistemas que guardan datos de los tarjetahabientes.			
1.3.9 Instalar software de cortafuego personal en cualquier computador móvil o de propiedad de los empleados con conectividad directa a Internet (por ejemplo, laptops que usan los empleados), mediante las cuales se acceda a la red de la organización.	**1.3.9** Verificar que los computadores móviles y de propiedad de los empleados con conectividad directa a Internet (por ejemplo, laptops utilizados por los empleados) que se usen para acceder a la red de la organización, tengan instalado y activado el software de cortafuego configurado por la organización de acuerdo con normas específicas, y que el mismo no pueda ser alterado por el empleado.			
1.4 Prohibir el acceso público directo entre redes externas y cualquier componente de sistema que guarde datos de los tarjetahabientes (por ejemplo, bases de datos).	**1.4** Para determinar que el acceso directo entre las redes públicas externas y los componentes de sistemas que guardan datos de los tarjetahabientes está prohibido, realizar las siguientes pruebas *específicamente* en la configuración de cortafuegos/ruteadores implementada entre el DMZ y la red interna:			
1.4.1 Implementar un DMZ para filtrar y controlar todo el tráfico y prohibir las rutas directas para el tráfico entrante y saliente de Internet.	**1.4.1** Examinar las configuraciones de cortafuego/ruteador y verificar que no hay ruta directa de entrada o salida para el tráfico de Internet.			
1.4.2 Restringir el tráfico saliente de	**1.4.2** Examinar las configuraciones de			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
las aplicaciones de tarjetas de pago a las direcciones de Internet (IP) dentro del DMZ.	cortafuegos/ruteadores y verificar que el tráfico interno de salida desde las aplicaciones de tarjetahabiente solamente puede acceder a direcciones de Internet (IP) dentro del DMZ.			
1.5 Implementar máscaras de IP para prevenir que las direcciones internas se traduzcan y revelen en Internet. Usar tecnologías que implementan el espacio de dirección RFC 1918 tales como Port Address Translation (PAT) o Network Address Translation (NAT).	**1.5** En la muestra de componentes de cortafuegos/ruteadores mencionados anteriormente, verificar que se use la tecnología NAT u otra tecnología que utilice el espacio de dirección RFC 1918 para restringir las transmisiones a direcciones de Internet (IP) desde la red interna hacia Internet (enmascaramiento de IP).			

Requisito 2: *No usar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.*

Los delincuentes que roban datos de computadores—comúnmente llamados “hackers” y que pueden ser externos o internos en una compañía—a menudo usan las contraseñas y otras opciones automáticamente programadas por los proveedores para comprometer la seguridad de los sistemas. Estas contraseñas y opciones son bien conocidas entre los delincuentes y fácilmente se determinan por medio de información pública.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
2.1 Cambiar siempre los valores por defecto de los proveedores **antes** de instalar un sistema en la red (por ejemplo, incluir contraseñas, cadenas comunitarias SNMP (Simple Network Management Protocol), y eliminar cuentas innecesarias).	**2.1** Elegir una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, e intentar establecer una conexión (con ayuda del administrador del sistema) con los dispositivos que usan las cuentas y contraseñas proporcionadas por los proveedores, a fin de verificar que los valores por defecto de las cuentas y contraseñas se han cambiado. (Use los manuales y sitios de los proveedores en Internet para obtener las cuentas y			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
	contraseñas automáticas que utilizan los proveedores.)			
2.1.1 En los ambientes inalámbricos, cambiar los valores por defecto programados por los vendedores del equipo inalámbrico, incluyendo, sin limitación, claves Wireless Equivalent Privacy (WEP), Service Set Identifier (SSID) de selección automática, contraseñas y cadenas comunitarias SNMP. Deshabilitar transmisiones SSID. Habilitar la tecnología Wi-Fi Protected Access (WPA y WPA2) para la encriptación y la autenticación cuando exista capacidad WPA.	**2.1.1** Verificar lo siguiente con respecto a los valores por defecto de los vendedores en los ambientes inalámbricos: • Las claves WEP se cambiaron en el momento de su instalación y se cambian en el momento en que una persona que tenga conocimiento de las mismas cesa en sus funciones o se traslada a otro puesto en la empresa. • Se cambió el valor por defecto de la SSID. • Se cambiaron las cadenas comunitarias SNMP en los puntos de acceso. • Se cambiaron las contraseñas por defecto en los puntos de acceso. • Se habilitó la tecnología WPA y WPA2 si el sistema inalámbrico tiene capacidad WPA. • Otras opciones y valores por defecto de los proveedores relacionados con la seguridad de los sistemas inalámbricos, según se aplique.			
2.2 Desarrollar normas de configuración para todos los componentes de sistemas. Asegurar que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y sean congruentes con las normas de alta seguridad aceptadas en la industria, por ejemplo, por SysAdmin Audit Network Security Networks (SANS), el National Institute of Standards Technology (NIST) y el Center for Internet Security (CIS).	**2.2.a** Examinar las normas de configuración de sistema de la organización para los componentes de red, servidores críticos, y puntos de acceso inalámbrico, y verificar que las normas de configuración de sistema son congruentes con las normas de alta seguridad aceptadas en la industria según lo definido por SANS, NIST y CIS.			
	2.2.b Verificar que las normas de configuración de sistema incluyen cada punto a continuación (2.2.1 – 2.2.4).			
	2.2.c Verificar que las normas de configuración de sistema se aplican al configurar nuevos sistemas.			
2.2.1 Implementar solamente una función primaria por cada servidor (por ejemplo, los servidores de Web, servidores de base de datos y DNS se	**2.2.1** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, verificar que solamente se ha implementado una función primaria por servidor.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
deben implementar en servidores separados).				
2.2.2 Deshabilitar todos los servicios y protocolos innecesarios (servicios y protocolos que no sean directamente necesarios para realizar la función especificada de los dispositivos).	**2.2.2** En una muestra de los componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, inspeccionar los servicios, daemons y protocolos habilitados. Verificar que los servicios o protocolos innecesarios o no seguros no estén habilitados o estén justificados y documentados en cuanto al uso apropiado del servicio (por ejemplo, FTP no se usa o se encripta con SSH u otra tecnología).			
2.2.3 Configurar los parámetros de seguridad del sistema para prevenir el uso indebido.	**2.2.3.a** Consultar con los administradores de sistema y/o gerentes de seguridad para determinar que tienen conocimiento de las programaciones comunes de parámetros de seguridad para sus sistemas operativos, servidores de base de datos, servidores de Web y sistemas inalámbricos.			
	2.2.3.b Verificar que las programaciones comunes de parámetros de seguridad están incluidas en las normas de configuración del sistema.			
	2.2.3.c En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, verificar que los parámetros de seguridad comunes se han establecido en forma apropiada.			
2.2.4 Eliminar todas las funcionalidades innecesarias, tales como archivos de comandos (scripts), accionadores, funciones, subsistemas, sistemas de archivos y servidores de Web innecesarios.	**2.2.4** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, verificar que todas las funcionalidades innecesarias (por ejemplo, archivos de comandos, accionadores, funciones, subsistemas, sistemas de archivo, etc.) se hayan eliminado. Igualmente, verificar que las funciones habilitadas estén documentadas, brinden soporte a una configuración segura y sean las únicas presentes en las máquinas incluidas en la muestra.			
2.3 Encriptar todo el acceso administrativo que no sea de consola. Usar tecnologías como SSH, VPN o SSL/TLS (Transport Layer Security)	**2.3** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, verificar que el acceso administrativo que no sea de consola está encriptado:			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
para la administración basada en Web y otros tipos de acceso administrativo sin consola.	• Observando a un administrador mientras se conecta con cada sistema incluido en la muestra, a fin de determinar que se invoca SSH (u otro método de encriptación) antes que se solicite la contraseña del administrador. • Revisando los archivos de servicio y parámetros en los sistemas incluidos en la muestra a fin de determinar que no están disponibles Telnet y otros comandos de conexión remota para uso interno. • Verificando que el acceso del administrador a la interfaz de administración inalámbrica está encriptado mediante SSL/TLS. Como alternativa, verificar que los administradores no se pueden conectar con la interfaz de administración inalámbrica (toda la administración de los ambientes inalámbricos se hace desde la consola).			
2.4 Los proveedores de servicio de hospedaje en redes deben proteger el ambiente hospedado y los datos de cada entidad. Estos proveedores deben cumplir con requisitos específicos detallados en el Apéndice A: "Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para los Proveedores de Servicios de Hospedaje en Redes."	**2.4** Realizar los procedimientos **A.1.1** a **A.1.4** detallados en el Apéndice A: "Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para los Proveedores de Servicios de Hospedaje en Redes" (con Procedimientos de Prueba) para las auditorías de **Proveedores de Hospedaje Compartido** de acuerdo con las normas mencionadas, a fin de verificar que dichos **Proveedores de Hospedaje Compartido** protegen el ambiente y los datos hospedados de las entidades a las cuales prestan servicio (comercios y proveedores de servicio).			

Proteger los Datos de los Tarjetahabientes

Requisito 3: Proteger los datos de los tarjetahabientes que están almacenados.

La encriptación es un componente crítico para la protección de los datos de los tarjetahabientes. Si un intruso subvierte otros controles de seguridad de red y obtiene acceso a los datos encriptados, sin las claves criptográficas no podrá leer ni utilizar esos datos. Otros métodos eficaces para proteger los datos almacenados deberían considerarse oportunidades potenciales para mitigar el riesgo. Por ejemplo, los métodos para minimizar el riesgo incluyen no guardar datos de los tarjetahabientes a menos que sea absolutamente necesario, truncar los datos de los tarjetahabientes si no se necesita el Número de Cuenta Primario (PAN) completo y no enviar el Número de Cuenta Primario en correos electrónicos no encriptados.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
3.1 Mantener el mínimo de datos de tarjetahabientes almacenados. Desarrollar una política de retención de datos y una política para disponer de los datos. Limitar la cantidad de datos almacenados y el tiempo de retención a los que se requieren para fines comerciales, legales y/o regulatorios, según se haya documentado en la política de retención de datos.	**3.1** Obtener y examinar las políticas y los procedimientos de la compañía sobre la retención y disposición de los datos y hacer lo siguiente: • Verificar que las políticas y procedimientos incluyen los requisitos legales, regulatorios y comerciales para la retención de los datos, incluyendo requisitos específicos para la retención de los datos de los tarjetahabientes (por ejemplo, es necesario mantener los datos de los tarjetahabientes durante X tiempo por X razones). • Verificar que las políticas y procedimientos incluyen requisitos para disponer de los datos cuando ya no se necesitan por razones legales, regulatorias o comerciales, incluyendo los datos de los tarjetahabientes. • Verificar que las políticas y procedimientos cubren todos los datos de los tarjetahabientes guardados, incluyendo servidores de base de datos, unidades mainframe, directorios de transferencia y directorios para copiar lotes de datos que se utilizan para transferir datos entre los servidores, y directorios utilizados para normalizar los datos entre transferencias de un servidor a otro. • Verificar que las políticas y los procedimientos incluyen			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
	un proceso de acceso programático (automático) para eliminar, al menos trimestralmente, los datos de los tarjetahabientes guardados que hayan excedido los requisitos comerciales de retención o, alternativamente, una auditoría, al menos trimestral, para verificar que los datos de los tarjetahabientes guardados no exceden los requisitos comerciales de retención.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
3.2 No almacenar datos de autenticación confidenciales después de la autorización (ni siquiera en forma encriptada). Los datos confidenciales de autenticación incluyen los datos citados en los Requisitos 3.2.1 a 3.2.3*:*	**3.2** Si se reciben y borran datos de autenticación confidenciales, obtener y revisar la metodología para borrar los datos, a fin de determinar que los mismos son irrecuperables. Por cada tipo de dato de autenticación confidencial a continuación, realice los siguientes pasos:			
3.2.1 No guardar el contenido íntegro de ninguna pista de banda magnética (en el reverso de una tarjeta, en un chip, o en cualquier otro lugar). Estos datos alternativamente se conocen como pista completa, pista 1, pista, pista 2 y datos de la banda magnética. *En el curso normal de los negocios es posible que sea necesario retener los siguientes elementos de datos de la banda magnética: el nombre del titular de la cuenta, el número de cuenta primario o PAN, la fecha de vencimiento y el código de servicio. A fin de minimizar el riesgo, guarde solamente aquellos elementos de datos que se necesiten por razones de negocio. NUNCA guarde el código de verificación de tarjeta o elementos de verificación de PIN.* *Nota: Vea el "Glosario" para obtener información adicional.*	**3.2.1** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, examinar lo siguiente y verificar que el contenido completo de cualquier pista de la banda magnética en el reverso de la tarjeta (datos del Valor de Verificación de Tarjeta) no se guarda bajo ninguna circunstancia: • Datos de transacción entrantes • Bitácoras y registros de transacciones • Archivos históricos • Archivos de rastreo • Bitácoras de *debugging* • Esquemas con varias bases de datos • Contenido de la base de datos			
3.2.2 No guardar el valor o código de validación de tarjeta (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de	**3.2.2** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, examinar lo siguiente y verificar que el código de validación de tres o cuatro dígitos impreso en el panel de			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
pago) utilizado para verificar las transacciones con tarjeta ausente. *Nota: Vea el "Glosario" para obtener información más detallada.*	firma de la tarjeta (datos del Valor de Verificación de Tarjeta, CVV2/CVC2) no se guarda bajo ninguna circunstancia: • Datos de transacción entrantes • Bitácoras y registros de transacciones • Archivos históricos • Archivos de rastreo • Bitácoras de *debugging* • Esquemas con varias bases de datos • Contenido de la base de datos			
3.2.3 No guardar el Número de Identificación Personal (PIN) o el bloque de PIN encriptado.	**3.2.3** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, examinar lo siguiente y verificar que los PINes y bloques de PIN encriptados no se guardan bajo ninguna circunstancia. • Datos de transacción entrantes • Bitácoras y registros de transacciones • Archivos históricos • Archivos de rastreo • Bitácoras de *debugging* • Esquemas con varias bases de datos • Contenido de la base de datos			
3.3 Enmascarar los números de cuenta cuando se desplieguen (los primeros seis y los últimos cuatro dígitos son el número máximo de dígitos que se puede desplegar). *(Note: Este requisito no se aplica a empleados y otras entidades que tienen específicamente necesidad de ver el Número de Cuenta Primario, ni sobresee los requisitos más estrictos establecidos para el despliegue de datos de los tarjetahabientes (por ejemplo, en recibos de terminales de punto de venta).*	**3.3** Obtener y examinar las políticas documentadas por escrito y revisar los despliegues en línea de datos de tarjetas de crédito, a fin de verificar que los números de las tarjetas de crédito se enmascaran al desplegar los datos de los tarjetahabientes, excepto en los casos en que existe una necesidad específica de ver el número de cuenta completo.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
3.4 Asegurar que el Número de Cuenta Primario (PAN), como mínimo, sea ilegible en cualquier lugar en que esté guardado (incluyendo datos en medios portátiles, medios de respaldo, registros o bitácoras, y datos recibidos de redes inalámbricas o guardados en las mismas) utilizando los siguientes métodos: • Funciones hash de una sola vía (índices hash) • Números truncados • Tokens de índice y pads (el pad debe ser guardado bajo seguridad) • Criptografía de alta seguridad como el estándar Triple-DES de 128 bits o el AES de 256 bits con procesos y procedimientos asociados de administración de claves. La información MÍNIMA sobre las cuentas que necesita estar en forma ilegible es el número de cuenta de la tarjeta de pago. *Si por alguna razón una compañía no puede encriptar los datos de los tarjetahabientes, consulte el Apéndice B: "Controles Compensatorios."*	**3.4.a** Obtener y examinar documentación acerca del sistema criptográfico utilizado para proteger los datos guardados, incluyendo el proveedor, el tipo de sistema/ proceso de criptografía y los algoritmos de encriptación (si se aplican). Verificar que los datos quedan ilegibles utilizando uno de los siguientes métodos: • Valores hash de una vía (hashed indexes) como el SHA-1 • Números truncados o máscara • Token de índice y PAD, y el PAD se guarda en forma segura • Criptografía de alta seguridad como Triple-DES de 128 bits o AES de 256 bits, con procesos y procedimientos de administración de claves asociados.			
	3.4.b Examinar varias tablas de una muestra de servidores de base de datos para verificar que los datos están encriptados (es decir, no están guardados en formato de texto en claro).			
	3.4.c Examinar una muestra de medios removibles (como cintas de respaldo) para confirmar que los datos de los tarjetahabientes se hacen ilegibles.			
	3.4.d Examinar una muestra de registros o bitácoras de auditoría para confirmar que los datos de los tarjetahabientes se sanean o eliminan de los registros.			
	3.4.e Verificar que todos los datos de los tarjetahabientes recibidos de las redes inalámbricas están encriptados dondequiera que se guardan.			
3.4.1 Si se usa la encriptación de discos (en lugar de la encriptación a nivel de archivo o columnas de base de datos) , el acceso lógico deberá administrarse	**3.4.1.a** Si se usa la encriptación en disco, verificar que el acceso lógico a los sistemas de archivos encriptados se ha implementado por medio de un mecanismo separado al mecanismo de los sistemas operativos nativos (por ejemplo, no se usan cuentas locales o del Directorio Activo).			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
independientemente de los mecanismos de control de acceso de los sistemas operativos nativos (por ejemplo, no usar las cuentas del sistema o Directorio Activo local). Las claves de decriptación no deberán estar vinculadas a las cuentas de usuarios.	**3.4.1.b** Verificar que las claves de decriptación no se guardan en el sistema local (por ejemplo, guardar claves en disquetes, CD-ROM, etc. y que están guardadas en forma segura para recuperarlas solamente cuando sea necesario).			
	3.4.1.c Verificar que los datos de los tarjetahabientes guardados en medios removibles están encriptados dondequiera que se guarden (la encriptación de disco frecuentemente no puede encriptar medios removibles).			
3.5 Proteger las claves (o llaves) de encriptación contra la divulgación y el uso indebido.	**3.5** Verificar los procesos para proteger las claves de encriptación contra la divulgación y uso indebido haciendo lo siguiente:			
3.5.1 Restringir el acceso a las claves y llaves al número mínimo de custodios necesarios.	**3.5.1** Examinar las listas de acceso de usuarios para determinar que el acceso a las claves criptográficas está restringido a unos cuantos custodios.			
3.5.2 Guardar las claves en forma segura en el mínimo número de ubicaciones y formatos posibles.	**3.5.2** Examinar los archivos de configuración de sistemas para verificar que las claves criptográficas se guardan en formato encriptado y que las claves de encriptación de claves se guardan separadas de otras claves de encriptación de datos.			
3.6 Documentar e implementar totalmente todos los procesos y procedimientos de administración de claves, incluyendo los siguientes:	**3.6.a** Verificar la existencia de procedimientos de administración de claves para las claves que se usan en la encriptación de datos de los tarjetahabientes.			
	3.6.b En el caso de los Proveedores de Servicio solamente: Si el Proveedor de servicio comparte claves con sus clientes para la transmisión de datos de los tarjetahabientes, verificar que dicho Proveedor de Servicio proporciona documentación a los clientes que incluye directrices sobre la forma en que pueden guardar y cambiar en forma segura las claves de encriptación de cliente (utilizadas para transmitir datos entre el cliente y el proveedor de servicio).			
	3.6.c Examinar los procedimientos de administración de claves y determinar que los mismos requieren lo siguiente:			
3.6.1 Generación de claves de alta seguridad	**3.6.1** Verificar que los procedimientos de administración de claves requieren la generación de claves de alta seguridad.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
3.6.2 Distribución segura de claves	**3.6.2** Verificar que los procedimientos de administración de claves requieren la distribución segura de las claves.			
3.6.3 Almacenamiento seguro de claves	**3.6.3** Verificar que los procedimientos de administración de claves requieren el almacenamiento seguro de las claves.			
3.6.4 Cambio periódico de claves • Según se considere necesario y lo recomiende la aplicación asociada (por ejemplo volver a digitar las claves), preferiblemente en forma automática • Al menos anualmente	**3.6.4** Verificar que los procedimientos de administración de claves requieren el cambio periódico de las claves. Verificar que los procedimientos de cambio de claves se realizan al menos anualmente.			
3.6.5 Destrucción de las claves viejas.	**3.6.5** Verificar que los procedimientos de administración de claves requieran la destrucción de las claves viejas.			
3.6.6 Establecer el conocimiento no compartido y el control dual de las claves de forma que se requiera a 2 o 3 personas, cada una de las cuales conozca solamente una parte de la clave, para reconstruir la clave completa.	**3.6.6** Verificar que los procedimientos de administración de claves requieran el conocimiento compartido y el control dual de las claves (de forma que se requiera a dos o tres personas, cada una de las claves conozca solamente una parte de la clave, para reconstruir la clave completa).			
3.6.7 Prevención de la sustitución no autorizada de las claves.	**3.6.7** Verificar que los procedimientos de administración de claves requieren prevenir que se sustituyan las claves en forma no autorizada.			
3.6.8 Reemplazo de claves cuando se sepa o sospeche que su seguridad ha sido comprometida.	**3.6.8** Verificar que los procedimientos de administración de claves requieran el reemplazo de claves cuando se sabe o sospecha que han sido comprometidas.			
3.6.9 Revocación de las claves viejas o inválidas	**3.6.9** Verificar que los procedimientos de administración de claves requieren la revocación de claves viejas o inválidas (primordialmente para las claves RSA).			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
3.6.10 Requisito de que los custodios de claves firmen un formulario especificando que comprenden y aceptan su responsabilidad como custodios de las claves.	**3.6.10** Verificar que los procedimientos de administración de claves requieren que los custodios de claves firmen un formulario especificando que comprenden y aceptan su responsabilidad como custodios de las claves.			

Requisito 4: *Encriptar los datos e información confidencial de los tarjetahabientes transmitida a través de redes públicas abiertas.*

La información confidencial debe encriptarse durante su transmisión a través de Internet, ya que es fácil y común que un delincuente intercepte y/o redirija los datos mientras se encuentran en tránsito.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
4.1 Usar criptografía y protocolos de alta seguridad como Secure Sockets Layer (SSL)/Transport Layer Security (TLS) e Internet Protocol Security (IPSEC) para salvaguardar los datos confidenciales de los tarjetahabientes durante su transmisión a través de redes públicas abiertas. *Ejemplos de redes públicas abiertas que caen dentro del alcance de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago son Internet, WiFi (IEEE 802.11x), Global System for Mobile Communications (GSM), y General Packet Radio Service (GPRS).*	**4.1.a** Verificar el uso de la encriptación (por ejemplo SSL/TLS o IPSEC) siempre que se transmitan o reciban a través de redes públicas abiertas. • Verificar que se usa la encriptación de alta seguridad durante la transmisión de datos. • En el caso de las implementaciones de SSL, verificar que HTTPS aparece como parte del URL (Universal Record Locator) del navegador y que no se requirió ningún dato de un tarjetahabiente cuando HTTPS no aparecía en el URL. • Seleccionar una muestra de transacciones según se reciban y observe las transacciones mientras ocurren para verificar que los datos de los tarjetahabientes se encriptan durante el tránsito. • Verificar que solamente se aceptan claves/ certificados SSL/TSL de confianza. • Verificar que se implementa la longitud apropiada de encriptación para la metodología que se está usando. (Consultar las recomendaciones y mejores prácticas de los suplidores/vendedores).			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
4.1.1 En el caso de las redes inalámbricas que transmitan datos de los tarjetahabientes, encriptar las transmisiones usando la tecnología Wi-Fi Protected Access (WPA o WPA2), IPSEC VPN, o SSL/TLS. Nunca depender exclusivamente de Wired Equivalent Privacy (WEP) para proteger el carácter confidencial y el acceso a una red de acceso local (LAN) inalámbrica. Si se usa WEP, hacer lo siguiente: • Usar con una clave de encriptación de un mínimo de 104 bits y valor de inicialización de 24 bits. • Usar SOLAMENTE en conjunción con la tecnología WiFi Protected Access (WPA o WPA2), VPN, o SSL/TLS. • Rotar trimestralmente (o automáticamente si la tecnología lo permite) las claves WEP compartidas. • Rotar las claves WEP compartidas siempre que haya cambios en el personal que tiene acceso a las claves. • Restringir el acceso basándose en la dirección de medios de código de acceso (MAC).	**4.1.1.a** En el caso de las redes inalámbricas que transmiten datos de los tarjetahabientes o están conectadas a otros ambientes donde están presentes estos datos, verificar que se usan las metodologías de encriptación apropiadas como Wi-FI Protected Access (WPA o WPA2), IPSEC, VPN o SSL/TLS.			
	4.1.1.b Si se usa WEP, verificar que: • se usa con una clave de encriptación de un mínimo de 104 bits y un valor de inicialización de 24 bits • se usa solamente en conjunción con la tecnología Wi-Fi Protected Access (WPA o WPA2), VPN, o SSL/TLS • las claves WEP compartidas se rotan al menos trimestralmente (o automáticamente si la tecnología tiene esta capacidad) • las claves WEP compartidas se rotan siempre que hay cambios en el personal que tiene acceso a las claves • el acceso está restringido basado en dirección MAC			
4.2 No enviar nunca información del tarjetahabiente por correo electrónico sin encriptar.	**4.2.a** Verificar que se usa una solución de encriptación de correo electrónico siempre que se envían datos de los tarjetahabientes por correo electrónico.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
	4.2.b Verificar la existencia de una política que establece que no se deberán enviar por correo electrónico Números de Cuenta Primarios sin encriptar.			
	4.2.c Consultar con 3-5 empleados para verificar que se requiere un software de encriptación para los mensajes de correo electrónico que contienen Números de Cuenta Primarios.			

Mantener un Programa de Manejo de Vulnerabilidad

Requisito 5: Usar y actualizar regularmente el software o programas antivirus.

Muchas vulnerabilidades y virus maliciosos y destructivos entran al sistema a través de la actividad de correo electrónico de los empleados. El software antivirus deberá utilizarse en todos los sistemas de correo electrónico y computadores de escritorio para proteger los sistemas de cualquier programación destructiva.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
5.1 Implementar software antivirus en todos los sistemas comúnmente afectados por virus (particularmente computadores personales y servidores). *Nota: Los sistemas comúnmente afectados por virus típicamente no incluyen los sistemas operativos basados en UNIX o mainframes.*	**5.1** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, verificar que hay software antivirus instalado.			
5.1.1 Asegurar que todos los programas antivirus sean capaces de detectar, eliminar y proteger contra otros tipos de softwares maliciosos y destructivos, incluyendo spyware y adware.	**5.1.1** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, verificar que los programas antivirus detectan, eliminan y protegen contra otros tipos de softwares maliciosos y destructivos, incluyendo spyware y adware.			

5.2 Asegurar que todos los mecanismos antivirus estén actualizados, estén funcionando activamente y sean capaces de generar registros y bitácoras de auditoría.	**5.2** Verificar que el software antivirus está actualizado, que opera activamente y es capaz de generar bitácoras o registros. • Obtener y examinar la política y verificar que contiene requisitos para actualizar el software antivirus y las definiciones. • Verificar que la instalación maestra del software está habilitada para ejecutar la actualización automática y escanes periódicos, y que los servidores examinados en la versión 5.1 y superior tienen activadas estas funciones. • Verificar que está activada la función de generación de bitácora y que los registros se están reteniendo de acuerdo con la política de retención de la empresa.			

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.

Las personas sin escrúpulos utilizan las vulnerabilidades en la seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad desarrollados por los proveedores. Todos los sistemas deben contar con estas actualizaciones de seguridad al software para estar protegidos contra la explotación por parte de empleados, delincuentes externos y virus. Nota: Los parches de software apropiados son aquellos que han sido suficientemente evaluados y probados para determinar que no crean conflicto con las configuraciones de seguridad existentes. En el caso de las aplicaciones desarrolladas internamente por la institución es posible evitar numerosas vulnerabilidades utilizando los procesos normales de desarrollo de sistemas y técnicas de codificación.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
6.1 Asegurar que todos los componentes de sistemas y software cuenten con los parches de seguridad más recientes proporcionados por los proveedores. Instalar los parches de seguridad relevantes dentro de un plazo de de un mes de publicados.	**6.1.a** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico y software relacionado, comparar la lista de parches de seguridad instalados en cada sistema a la lista de parches de seguridad más reciente del proveedor, a fin de determinar que están instalados los parches actualizados.			
	6.1.b Examinar las políticas relacionadas con la instalación de parches de seguridad a fin de determinar que requieren instalación de todos los nuevos parches de seguridad relevantes dentro de un plazo de 30 días.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
6.2 Establecer un proceso para identificar las vulnerabilidades de seguridad recientemente descubiertas (por ejemplo, suscribirse a los servicios de alerta disponibles en forma gratuita a través de Internet). Actualizar sus normas para subsanar cualquier nuevo problema de vulnerabilidad que pudiera surgir.	**6.2.a** Consultar con el personal responsable para verificar que hay procesos implementados para identificar nuevas vulnerabilidades de seguridad.			
	6.2.b Verificar que los procesos para identificar nuevas vulnerabilidades de seguridad incluyen el uso de fuentes externas de información sobre vulnerabilidades de seguridad y actualizar los estándares de configuración de sistemas revisados en el Requisito 2 a medida que se encuentren problemas de vulnerabilidad.			
6.3 Desarrollar aplicaciones de software basadas en las mejores prácticas de la industria e incorporar la seguridad de la información a través de todo el ciclo de desarrollo de software.	**6.3** Obtener y examinar los procesos de desarrollo de software documentados por escrito para confirmar que se basan en las normas de la industria y que se contempla la seguridad durante todo el ciclo de vida. A partir de la revisión de los procesos de desarrollo de software documentados, preguntar a los que desarrollan los programas y revisar los datos relevantes (documentación de la configuración de redes, producción y datos de prueba, etc.) para verificar que:			
6.3.1 Hacer pruebas de todos los parches de seguridad y cambios de configuración de software y sistema antes de implementar.	**6.3.1** Todos los cambios (incluyendo parches) se prueban antes de implementarlos para producción.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
6.3.2 Separar los ambientes de desarrollo, prueba y producción.	**6.3.2** Los ambientes de prueba y desarrollo son separados del ambiente de producción, con control de acceso establecido para hacer cumplir esa separación.			
6.3.3 Separar las responsabilidades entre los ambientes de desarrollo y prueba y producción.	**6.3.3** Existe una separación de responsabilidades entre las del personal asignado a los ambientes de desarrollo/prueba y las del personal asignado al ambiente de producción.			
6.3.4 Los datos de producción (números reales de cuentas de tarjetas) no se usan para fines de prueba y desarrollo.	**6.3.4** Los datos utilizados para probar y desarrollar los ambientes y verificar que los datos de producción (números reales de tarjetas de crédito) no se usan para fines de prueba y desarrollo o se sanean antes de utilizarlos.			
6.3.5 Eliminar todos los datos y cuentas de prueba antes de activar los sistemas de producción.	**6.3.5** Los datos y cuentas de prueba se eliminan antes de activar un sistema de producción.			
6.3.6 Eliminar las cuentas, nombres de usuarios y contraseñas de aplicaciones individuales antes que las aplicaciones se activen o se pongan a disposición de los clientes.	**6.3.6** Las cuentas, nombres de usuario y contraseñas individuales se eliminan del sistema al entrar el mismo en producción o ponerse a disposición de los clientes.			
6.3.7 Revisar los códigos individuales antes de ponerlos en producción o a disposición de los clientes, a fin de identificar cualquier vulnerabilidad relacionada con la codificación.	**6.3.7.a** Obtener y revisar las políticas documentadas por escrito para confirmar que establecen el requisito de revisar los códigos y de que la revisión sea realizada por personas que no sean el autor del código.			
	6.3.7.b Verificar que se revisan los códigos cuando se agregan nuevos códigos o se hacen cambios. *Nota: Este requisito se aplica a las revisiones de códigos para desarrollo de software individual como parte del Ciclo de Vida de Desarrollo de Sistema (System Development Life Cycle, SDLC). Estas revisiones las puede realizar el personal interno. Los códigos individuales de las aplicaciones conectadas a la Web estarán sujetos a controles adicionales con vigencia el 30 de junio de 2008. Vea el Requisito 6.6 de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para obtener información detallada.*			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
6.4 Seguir los procedimientos de control de cambios para todas las modificaciones de configuración de sistemas y software. Los procedimientos deben incluir lo siguiente:	**6.4.a** Obtener y examinar los procedimientos de cambio de control relacionados con la implementación de los parches de seguridad y las modificaciones de software y determinar que los procedimientos requieren los puntos **6.4.1** – **6.4.4** a continuación.			
	6.4.b En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, examinar los tres cambios o parches de seguridad más recientes de cada componente de sistema y rastrear esos cambios a la documentación relacionada con los controles de cambios. Verificar que por cada cambio examinado se documentó lo siguiente de acuerdo con los procedimientos de control de cambios:			
6.4.1 Documentación del impacto	**6.4.1** Verificar que la documentación del impacto para el cliente está incluida en la documentación de control de cambios de cada cambio incluido en la muestra.			
6.4.2 Aprobación final por escrito (con firma) de los funcionarios apropiados	**6.4.2** Verificar que se recibió aprobación de la administración firmada por cada funcionario apropiado para cada cambio incluido en la muestra.			
6.4.3 Pruebas de funcionalidad operativa	**6.4.3** Verificar que se realizaron las pruebas para verificar la funcionalidad operativa en cada cambio incluido en la muestra.			
6.4.4 Procedimientos de cancelación	**6.4.4** Verificar que se prepararon procedimientos de cancelación para cada cambio incluido en la muestra.			
6.5 Desarrollar todas las aplicaciones de Web tomando como base las directrices de codificación segura como *Open Web Application Security Project Guidelines*. Revisar el código de aplicación individual para identificar vulnerabilidades de codificación. ." Contemplar la prevención de vulnerabilidades comunes de codificación en los procesos de desarrollo de software, que incluyen	**6.5.a** Obtener y examinar los procesos de desarrollo de software de todas las aplicaciones basadas en Web. Confirmar que los procesos requieren capacitación sobre las técnicas seguras de codificación para los programadores y está basado en guías como las directrices OWASP *(OWASP Guidelines,* http://www.owasp.org)			
	6.5.b En el caso de cualquier aplicación basada en Web, determinar que se han establecido procesos para constatar que las aplicaciones de Web no están vulnerables a lo siguiente:			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
las siguientes:				
6.5.1 Ingreso de datos sin validar	**6.5.1** Ingreso de datos sin validar			
6.5.2 Control de acceso interrumpido (por ejemplo, uso malicioso de las identificaciones de usuarios).	**6.5.2** Uso malicioso de las ID de usuario.			
6.5.3 Interrupción de la autenticación o administración de sesiones (uso de credenciales de cuenta y cookies de sesión).	**6.5.3** Uso malicioso de las credenciales de cuentas y cookies de sesión.			
6.5.4 Ataques con inyección de códigos en ventanas pertenecientes a diferentes dominios (el llamado Cross-Site Scripting o XSS).	**6.5.4** Archivos de comandos de ventanas pertenecientes a diferentes dominios (Cross-site scripting).			
6.5.5 Ataques de buffer overflow.	**6.5.5** Buffer overflows debidos a datos de entrada no validados y otras causas.			
6.5.6 Defectos de inyección (por ejemplo, inyección de Structured Query Language, SQL).	**6.5.6** Inyección de SQL y otros defectos de inyección de comandos.			
6.5.7 Manejo inapropiado de errores.	**6.5.7** Defectos en el manejo de errores.			
6.5.8 Almacenaje sin la debida seguridad.	**6.5.8** Almacenaje no seguro.			
6.5.9 Negación de servicio.	**6.5.9** Negación de servicio.			
6.5.10 Administración no segura de configuraciones.	**6.5.10** Administración de configuración que no es segura.			
6.6 Asegurar que todas las aplicaciones hacia la Web estén protegidas contra ataques conocidos	**6.6** En el caso de las aplicaciones hacia la Web, asegurar que está establecido uno de los siguientes métodos: • Verificar que una organización especializada en			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
mediante cualquiera de los siguientes métodos: • Haciendo que una organización especializada en seguridad de aplicaciones revise todos los códigos individuales de aplicación para eliminar vulnerabilidades comunes. • Instalando un cortafuego a nivel de capa de aplicación frente a las aplicaciones conectadas a la Web. *Nota: Este método está considerado una mejor práctica hasta el 30 de junio de 2008, y después de esta fecha se convierte en requisito.*	seguridad de aplicaciones revisa periódicamente el código de aplicación individual y que se han corregido todas las vulnerabilidades de codificación, así como que la aplicación fue reevaluada después de hacer las correcciones. • Verificar que hay un cortafuego a nivel de capa de aplicación frente a todas las aplicaciones conectadas a la Web para detectar y prevenir ataques provenientes de la misma.			

Implementar Medidas Sólidas de Control de Acceso

Requisito 7: Restringir el acceso a los datos de los tarjetahabientes tomando como base la necesidad del funcionario de conocer la información.

Este requisito asegura que sólo el personal autorizado tenga acceso a los datos críticos.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
7.1 Limitar el acceso a los recursos de computación y a la información de los tarjetahabientes exclusivamente a aquellas personas que por necesidad de su trabajo requieran dicho acceso.	**7.1** Obtener y examinar la política documentada por escrito de control de datos y verificar que la misma incluye lo siguiente: • Los derechos de acceso de las ID de Usuario privilegiadas están restringidos a los privilegios mínimos necesarios para realizar el trabajo. • La asignación de privilegios a las personas se basa en la clasificación y función de trabajo. • Requisito de un formulario de autorización que firma la administración y especifica los privilegios requeridos. • Implementación de un sistema automatizado de control de acceso.			
7.2 Establecer un mecanismo para los sistemas de múltiples usuarios que restrinja el acceso tomando como base la necesidad del usuario de conocer la información y esté programado para negar el acceso a todo el mundo, a menos que esté permitido específicamente.	**7.2** Examinar las programaciones de los sistemas y la documentación de los proveedores para verificar que se ha establecido un sistema de control de acceso y que el mismo incluye lo siguiente: • Cobertura de todos los componentes de sistema. • Asignación de privilegios a personas basada en la clasificación y función de trabajo. • Sistema programado para negar automáticamente todos los accesos (algunos sistemas están programados automáticamente para permitir todos los accesos a menos que se escriba una regla específicamente para negar el acceso o hasta que exista dicha regla).			

Requisito 8: Asignar una identificación única a cada persona que tenga acceso a un computador.

Asignar una identificación (ID) única a cada persona que tenga acceso asegura que las acciones tomadas con respecto a datos y sistemas críticos sean realizadas por usuarios conocidos y autorizados y que las mismas puedan ser rastreadas.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
8.1 Identificar a todos los usuarios mediante un nombre de usuario único antes de permitirles el acceso a los componentes de sistemas y datos de los tarjetahabientes.	**8.1** En una muestra de identificaciones de usuarios, revisar las listas de ID de usuario y verificar que todos los usuarios tengan un nombre de usuario único para el acceso a los componentes de sistemas o datos de los tarjetahabientes.			
8.2 Además de asignar una ID de usuario única, emplear al menos uno de los métodos enumerados a continuación para autenticar a todos los usuarios: • Contraseña • Dispositivos de token (por ejemplo, SecureID, certificados o clave pública) • Biométrica	**8.2** Para verificar la autenticación de los usuarios mediante una ID única de usuario y otro medio de autenticación adicional (por ejemplo, contraseña) para el acceso al ambiente de los tarjetahabientes, hacer lo siguiente: • Obtener y examinar documentación que describa el método o los métodos de autenticación que se utilizan. • En el caso de cada método de autenticación utilizado y una vez en el caso de cada componente de sistema, observar una autenticación para verificar que el proceso de autenticación está funcionando de acuerdo con el método o los métodos de autenticación documentados.			
8.3 Implementar la autenticación de 2 factores para el acceso remoto a la red por parte de los empleados, administradores y terceros. Usar tecnologías como Remote Authentication and Dial-In Service (RADIUS) o Terminal Access Controller Access Control System (TACACS) con tokens, o VPN (basado en SSL/TLS o IPSEC) con certificados individuales.	**8.3** Para determinar que está establecida la autenticación de 2 factores en todos los accesos remotos a la red, observar a un empleado (por ejemplo, a un administrador) mientras se conecta remotamente a la red y verificar que se requieren tanto una contraseña como otro medio de autenticación (tarjeta inteligente, token de PIN, etc.).			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
8.4 Encriptar todas las contraseñas durante la transmisión y el almacenaje, en todos los componentes de sistemas.	**8.4.a** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, examinar los archivos de contraseñas para verificar que no se pueden leer las contraseñas.			
	8.4.b En el caso de los **Proveedores de Servicio** solamente, observar los archivos de contraseñas para verificar que las contraseñas de los clientes están encriptadas.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
8.5 Asegurar la autenticación apropiada de los usuarios y la administración correcta de las contraseñas de los usuarios y administradores en todos los componentes de sistemas de la manera siguiente:	**8.5** Revisar los procedimientos y consultar con el personal para verificar que se han implementado procedimientos para la autenticación de usuarios y administración de contraseñas haciendo lo siguiente:			
8.5.1 Controlar la adición, eliminación y modificación de las identificaciones de usuarios, credenciales y otros objetos de identificación.	**8.5.1.a** Seleccionar una muestra de las ID de usuario, incluyendo administradores y usuarios generales. Verificar que cada usuario está autorizado para usar el sistema de acuerdo con las políticas de la compañía haciendo lo siguiente: • Obtener y examinar un formulario de autorización para cada ID. • Verificar que las ID de la muestra se hayan implementado de acuerdo con el formulario de autorización (incluyendo los privilegios especificados y después de obtener todas las firmas) rastreando el formulario de autorización al sistema.			
	8.5.1.b Verificar que sólo los administradores tienen acceso a las consolas de administración de las redes inalámbricas.			
8.5.2 Verificar la identidad del usuario antes de reprogramar (reset) las contraseñas.	**8.5.2** Examinar los procedimientos de contraseña y observar al personal de seguridad para confirmar que, si un usuario solicita la reprogramación de una contraseña por teléfono, correo electrónico, Web u otro método que no sea cara a cara, la identidad del usuario se verifica antes que se reprograme la contraseña.			
8.5.1 Programar la primera contraseña de un usuario a un valor único para dicho usuario y cambiarla inmediatamente después del primer uso.	**8.5.3** Examinar los procedimientos de contraseña y observar al personal de seguridad para confirmar que las contraseñas establecidas por primera vez para los nuevos usuarios se programan a un valor único por usuario, y que las mismas se cambian después del primer uso.			
8.5.4 Revocar inmediatamente el acceso de todo usuario que ya no sea un empleado o no lo requiera.	**8.5.4** Seleccionar una muestra de empleados que hayan cesado en sus funciones durante los últimos 6 meses y revisar los listados de acceso de usuarios para verificar que sus ID se han deshabilitado o eliminado.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
8.5.5 Eliminar las cuentas de usuarios inactivos al menos cada 90 días.	**8.5.5** En una muestra de ID de usuarios, verificar que no hay cuentas inactivas de más de 90 días.			
8.5.6 Habilitar cuentas para uso de los proveedores para mantenimiento remoto solamente durante el tiempo necesario.	**8.5.6** Verificar que cualquier cuenta utilizada por los proveedores para brindar soporte y mantener los componentes de sistemas está inactiva, se habilita solamente cuando el proveedor la necesita y se supervisa mientras se está usando.			
8.5.7 Comunicar los procedimientos y políticas relacionadas con las contraseñas a todos los usuarios que tengan acceso a la información de los tarjetahabientes.	**8.5.7** Consultar con los usuarios de una muestra de IDs de usuario para verificar que están familiarizados con los procedimientos y políticas concernientes a las contraseñas.			
8.5.8 No usar cuentas o contraseñas grupales, compartidas o genéricas.	**8.5.8.a** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, examinar las listas de ID de usuario para verificar lo siguiente: • Las ID y cuentas genéricas se deshabilitan o eliminan. • No existen ID compartidas para las actividades de administración de sistemas y otras funciones críticas. • No se usan ID compartidas y genéricas para administrar las redes de acceso local (LAN) y dispositivos inalámbricos.			
	8.5.8.b Examinar los procedimientos y políticas para verificar que las contraseñas grupales y compartidas están explícitamente prohibidas.			
	8.5.8.c Consultar con los administradores de sistema para verificar que las contraseñas de grupo y compartidas están explícitamente prohibidas.			
8.5.9 Cambiar la contraseña de los usuarios al menos cada 90 días.	**8.5.9** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, obtener e inspeccionar las programaciones de configuración de sistema para verificar que los parámetros de contraseña están programados para requerir a los			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
	usuarios cambiar las contraseñas como mínimo cada 90 días. En el caso de los **Proveedores de Servicio**, revisar los procesos internos y la documentación de los clientes/usuarios para verificar que se requiere cambiar periódicamente las contraseñas de clientes y que se da a los clientes una guía con respecto a cuándo y bajo qué circunstancias deberían cambiarse las contraseñas.			
8.5.10 Requerir una longitud mínima de contraseña de al menos siete caracteres.	**8.5.10** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, obtener e inspeccionar las programaciones de configuración de sistema para verificar que los parámetros de contraseña están programados para requerir que la contraseña tenga al menos siete caracteres. En el caso de los Proveedores de Servicio solamente, revisar los procesos internos y la documentación de los clientes/usuarios para verificar que se requiere que las contraseñas de clientes cumplan con los requisitos de longitud mínima.			
8.5.11 Usar contraseñas que contengan tanto caracteres numéricos como alfabéticos.	**8.5.11** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, obtener e inspeccionar las programaciones de configuración de sistema para verificar que los parámetros de contraseña están establecidos para requerir que las contraseñas contengan tanto caracteres numéricos como alfabéticos. En el caso de los **Proveedores de Servicio** solamente, revisar los procesos internos y la documentación de clientes/usuarios para verificar que se requiere que las contraseñas de los clientes contengan tanto caracteres numéricos como alfabéticos.			
8.5.12 No permitir a ninguna persona que presente una nueva contraseña que sea igual que cualquiera de las últimas cuatro que ha utilizado.	**8.5.12** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, obtener e inspeccionar las programaciones de configuración de sistema para verificar que los parámetros de contraseña están establecidos para requerir que las nuevas contraseñas no pueden ser iguales a las cuatro contraseñas previamente utilizadas. En el caso de los **Proveedores de Servicio** solamente, revisar los procesos internos y la documentación de los clientes/usuarios para verificar que las nuevas contraseñas de los clientes no pueden ser iguales a las cuatro contraseñas previas.			
8.5.13 Limitar los intentos	**8.5.13**En una muestra de componentes de sistemas, servidores			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
repetidos de lograr acceso bloqueando la ID del usuario después de un máximo de seis intentos.	críticos y puntos de acceso inalámbrico, obtener e inspeccionar las programaciones de configuración de sistema para verificar que los parámetros de contraseñas están establecidos para requerir que la cuenta de un usuario se bloquee después de un máximo de seis intentos inválidos de conexión. En el caso de los **Proveedores de Servicio** solamente, revisar los procesos internos y la documentación de los clientes/usuarios para verificar que las cuentas de los clientes se bloquean temporalmente después de un máximo de seis intentos inválidos de obtener acceso.			
8.5.14 Programar la duración de este bloqueo a treinta minutos o hasta que el administrador del sistema habilite la ID del usuario.	**8.5.14** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, obtener e inspeccionar las programaciones de configuración de sistema para verificar que se programan parámetros de contraseña para requerir que una vez que se bloquee una cuenta de usuario, la misma se mantengan bloqueada por treinta minutos o hasta que un administrador de sistema reprograme la cuenta.			
8.5.15 Si no ha habido actividad en una sesión durante más de 15 minutos, requerir que el usuario vuelva a ingresar la contraseña para reactivar el terminal.	**8.5.15** En una muestra de componentes de sistemas, servidores críticos y puntos de acceso inalámbrico, obtener e inspeccionar las programaciones de configuración de sistema para verificar que la función de interrupción automática de sistema o sesión por inactividad ("timeout") se ha programado a 15 minutos o menos.			
8.5.16 Autenticar todos los accesos a cualquier base de datos que contenga información de los tarjetahabientes. Esto incluye acceso por parte de las aplicaciones, los administradores y todos los demás usuarios.	**8.5.16.a** Revisar las programaciones de configuración de base de datos de una muestra de bases de datos para verificar que el acceso se autentica, incluyendo el de las personas, aplicaciones y administradores.			
	8.5.16.b Revisar las programaciones de configuración y las cuentas de bases de datos para verificar que las consultas directas SQL a la base de datos estén prohibidas (debe haber muy pocas cuentas individuales de conexión de base de datos, limitadas a los administradores de base de datos). Las consultas directas de SQL deben limitarse a los administradores de base de datos).			

Requisito 9: Restringir el acceso físico a los datos de los tarjetahabientes.

Cualquier acceso físico a los datos o sistemas que contienen datos de los tarjetahabientes brinda una oportunidad de acceder a dispositivos o datos y eliminar sistemas o copias impresas, y debe ser restringido de forma apropiada.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
9.1 Usar controles apropiados de entrada a las instalaciones para limitar y monitorear el acceso a los sistemas que almacenan, procesan o transmiten datos de los tarjetahabientes.	**9.1** Verificar la existencia de los siguientes controles de seguridad física en cada salón de computadores, centro de datos y otras áreas físicas donde existan sistemas que contienen datos de los tarjetahabientes: • Verificar que el acceso está controlado por lectores de gafetes y otros dispositivos, incluyendo gafetes autorizados y llave y candado. • Observar a un administrador de sistema mientras intenta conectarse con las consolas de tres sistemas seleccionados aleatoriamente en el ambiente de datos de los tarjetahabientes y verificar que los mismos están “bloqueados” para prevenir el uso no autorizado.			
9.1.1 Usar cámaras para vigilar las áreas vulnerables. Auditar estos datos y correlacionar con otros. Guardar durante al menos tres meses, a menos que existan otras restricciones impuestas por la ley.	**9.1.1** Verificar que las cámaras de video vigilan los puntos de entrada y salida de los centros de datos donde se guardan o se mantienen datos de los tarjetahabientes. Las cámaras de video deben ser internas en los centros de datos o deben estar protegidas de alguna otra manera de la alteración o desactivación. Verificar que las cámaras están supervisadas y que los datos de las mismas se guardan durante al menos tres meses.			
9.1.2 Restringir el acceso físico a los conectores de redes (network jacks) accesibles al público.	**9.1.2** Verificar mediante consultas con los administradores de sistemas y observación que las conexiones físicas con las redes están habilitadas solamente cuando son necesarias para los empleados autorizados. Por ejemplo, los salones de conferencia utilizados para recibir a los visitantes no deben tener puertos de red habilitados con DHCP. Como alternativa, verificar que los visitantes están acompañados en todo momento en las áreas donde hay conexiones activas.			
9.1.3 Restringir el acceso físico a los puntos de acceso inalámbrico,	**9.1.3** Verificar que el acceso físico a los puntos de acceso inalámbrico, pasarelas y dispositivos de mano (handheld) está			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
pasarelas y dispositivos de mano (handheld).	restringido de forma apropiada.			
9.2 Desarrollar procedimientos para ayudar al personal a distinguir fácilmente a los empleados de los visitantes en las áreas en que la información de los tarjetahabientes está accesible. *"Empleado" se refiere a los funcionarios que laboran a jornada completa o parcial, empleados y personal temporal y consultores "residentes" en la ubicación. Un "visitante" es un proveedor, invitado de un funcionario o cualquier otra persona que entre a las instalaciones durante un período breve, normalmente* no más de un día.	**9.2.a** Revisar los procesos y procedimientos para asignar gafetes e identificaciones a los empleados, contratistas y visitantes, y verificar que estos procesos incluyen: • Procesos para emitir nuevos gafetes, requisitos para cambiar el acceso y revocar los privilegios de los empleados que cesan en sus funciones y gafetes de visitantes que ya han caducado. • Acceso limitado al sistema de emisión de gafetes e identificaciones.			
	9.2.b Observar a las personas que se encuentran en las instalaciones para determinar que es fácil distinguir entre los empleados y los visitantes.			
9.3 Asegurar que se haga lo siguiente en el caso de todos los visitantes:	**9.3** Verificar que se han establecido controles para empleados/visitantes de la manera siguiente:			
9.3.1 Sean autorizados antes de entrar a las áreas donde se procesa o mantiene la información de los tarjetahabientes.	**9.3.1** Observar a los visitantes para verificar el uso de los gafetes e identificaciones. Intentar obtener acceso al centro de datos para verificar que el gafete del visitante no le permite entrar sin un acompañante a las áreas donde se guardan los datos de los tarjetahabientes.			
9.3.2 Reciban una identificación física (gafete o dispositivo de acceso) que caduque y que los identifique como personas que no son empleados.	**9.3.2** Examinar los gafetes e identificaciones de los empleados y visitantes para verificar que los de los visitantes los distinguen claramente de los empleados y personas ajenas y que las identificaciones de los visitantes caducan.			
9.3.3 Entreguen su identificación física antes de salir de las	**9.3.3** Observar a los visitantes que salen de las instalaciones para verificar que se les pide que entreguen su identificación al			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
instalaciones o en la fecha en que caduque la misma.	salir o en la fecha de caducación.			
9.4 Usar un registro de visitas para mantener una bitácora física de la actividad de visitas. Retener este registro por un mínimo de tres meses, a menos que existan otras restricciones impuestas por la ley.	**9.4.a** Verificar que se usa un registro de visitantes para controlar el acceso físico a las instalaciones, así como en los salones de computadores y centros de datos donde se guarda o transmite información de los tarjetahabientes.			
	9.4.b Verificar que el registro contiene el nombre del visitante, la empresa representada y el nombre del empleado que autoriza el acceso físico, y que dicho registro se retiene durante al menos 3 meses.			
9.5 Guardar las copias de respaldo en un lugar seguro fuera de las instalaciones, que puede ser las instalaciones de un tercero o un almacenaje comercial.	**9.5** Verificar que la ubicación para almacenar los respaldos es segura. Verificar que cualquier almacenaje fuera de las instalaciones se visita periódicamente para determinar que los medios de respaldo están físicamente seguros y a prueba de incendios.			
9.6 Asegurar físicamente todos los medios electrónicos y en papel (es decir, computadores, medios electrónicos y hardware de redes y comunicaciones, líneas de telecomunicaciones, recibos en papel, reportes impresos y telefacsímiles) que contengan información de los tarjetahabientes.	**9.6** Verificar que los procedimientos para proteger los datos de los tarjetahabientes incluyen controles para asegurar físicamente las copias impresas y los medios electrónicos en los salones de computadores y centros de datos (incluyendo los recibos, reportes y telefacsímiles en papel, CD y discos guardados en los escritorios de los empleados y espacios abiertos, y discos duros de los computadores).			
9.7 Mantener un control estricto de la distribución interna y externa de cualquier tipo de medio que contenga información de los tarjetahabientes.	**9.7** Verificar que existe una política para controlar la distribución de la información del tarjetahabiente, que cubre todos los medios distribuidos, incluyendo los que se distribuyen a personas.			
9.7.1 Clasificar los medios para que puedan ser identificados como confidenciales.	**9.7.1** Verificar que todos los medios están clasificados para que se puedan identificar como “confidenciales”.			
9.7.2 Enviar los medios a través de un servicio de mensajería o mecanismo de entrega seguro que	**9.7.2** Verificar que todos los medios enviados fuera de las instalaciones se documentan en un registro y son autorizados por la administración, y que se envían a través de un servicio de			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
pueda rastrearse en forma precisa.	mensajería seguro u otro mecanismo de entrega que se puede rastrear.			
9.8 Asegurar que la administración apruebe todos los medios que se trasladen desde áreas seguras (particularmente cuando estos medios se distribuyan a personas).	**9.8** Seleccionar una muestra reciente de registros de rastreo de medios en instalaciones externas por varios días y verificar que contienen los detalles apropiados de registro y la autorización apropiada de la administración.			
9.9 Mantener un control estricto del almacenaje y accesibilidad de los medios que contengan información de los tarjetahabientes.	**9.9** Obtener y examinar la política para controlar el almacenaje y mantenimiento de copias impresas y medios electrónicos y verificar que esta política requiere inventarios periódicos de los medios.			
9.9.1 Mantener un inventario apropiado de todos los medios y asegurar que los mismos estén almacenados en forma segura.	**9.9.1.a** Obtener y revisar el registro de inventario de medios para verificar que se están realizando periódicamente los inventarios de medios. **9.9.1.b** Obtener y revisar los procesos establecidos para verificar que los medios se almacenan en forma segura.			
9.10 Destruir los medios que contengan información de los tarjetahabientes cuando ya no sean necesarios para el negocio o por razones legales:	**9.10** Obtener y examinar la política de destrucción de medios y verificar que cubre todos los medios que contienen datos de los tarjetahabientes y confirmar lo siguiente.			
9.10.1 Pasar los materiales impresos por una trituradora que corte en zig zag o reducirlos a pulpa.	**9.10.1.a** Verificar que los materiales impresos se hayan pasado por la trituradora en zig zag, incinerado o reducido a pulpa, de acuerdo con las normas ISO 9564-1 o ISO 11568-3e.			
	9.10.1.b Examinar los contenedores de almacenaje de información para verificar que los mismos son seguros. Por ejemplo, verificar que un contenedor con materiales para pasar por la trituradora tenga candado y llave, a fin de prevenir el acceso al contenido.			
9.10.2 Purgar, borrar electrónicamente, triturar o de otra manera destruir los medios electrónicos para que los datos de los tarjetahabientes no se puedan	**9.10.2** Verificar que los medios electrónicos se destruyen más allá de toda posibilidad de recuperación utilizando un programa de borrado militar para borrar los archivos y por medio de borrado electrónico o destruyendo físicamente de otra forma los medios.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
reconstruir.				

Monitorear y Probar Regularmente las Redes

Requisito 10: *Rastrear y monitorear todo el acceso a los recursos de la red y datos de los tarjetahabientes.*

Los mecanismos de conexión y la capacidad de rastrear las actividades de los usuarios son críticos. La presencia de registros o bitácoras en todos los ambientes permite un rastreo y análisis detallados cuando algo marcha mal. Determinar la causa de un compromiso de seguridad es una tarea muy difícil cuando el sistema no cuenta con registros de actividad.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
10.1 Establecer un proceso para vincular todos los accesos a componentes del sistema (particularmente aquellos realizados con privilegios administrativos - root) a un usuario individual.	**10.1** Verificar por medio de la observación y consulta con el administrador del sistema que se han habilitado bitácoras de auditoría y que las mismas están activas, incluyendo las de todas las redes inalámbricas conectadas.			
10.2 Implementar bitácoras de auditoría automatizadas para reconstruir los siguientes eventos en todos los componentes de sistemas:	**10.2** Confirmar por medio de consultas, revisiones de los registros de auditoría y revisión de las programaciones de registros de auditoría, que los siguientes eventos se han registrado en las bitácoras de actividad del sistema:			
10.2.1 Todos los accesos a los datos de los tarjetahabientes por parte de un usuario individual.	**10.2.1** Todos los accesos a los datos de los tarjetahabientes por parte de un usuario individual.			
10.2.2 Todas las acciones de cada persona con privilegios root o administrativos.	**10.2.2** Acciones tomadas por cualquier persona que tenga privilegios root o administrativos.			
10.2.3 Acceso a todas las bitácoras de	**10.2.3** Acceso a todas las bitácoras de auditoría.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
auditoría.				
10.2.4 Intentos inválidos para lograr un acceso lógico.	**10.2.4** Intentos inválidos para lograr un acceso lógico.			
10.2 5 Uso de mecanismos de identificación y autenticación.	**10.2.5** Uso de mecanismos de identificación y autenticación.			
10.2.6 Inicialización de los registros o bitácoras de auditoría.	**10.2.6** Inicialización de los registros o bitácoras de auditoría.			
10.2.7 Creación y eliminación de todos los objetos a nivel de sistema.	**10.2.7** Creación y eliminación de todos los objetos a nivel de sistema.			
10.3 Registrar al menos las siguientes bitácoras de auditoria en todos los componentes del sistema para cada evento:	**10.3** Verificar por medio de consultas y de la observación, para cada evento auditable (desde 10.2), que la bitácora de auditoría captura lo siguiente:			
10.3.1 Identificación de usuario	**10.3.1** Identificación del usuario			
10.3.2 Tipo de evento	**10.3.2** Tipo de evento			
10.3.3 Fecha y hora	**10.3.3** Sello de fecha y hora			
10.3.4 Éxito o fallo	**10.3.4** Señal de éxito o fracaso, incluyendo las de las conexiones inalámbricas.			
10.3.5 Origen del evento	**10.3.5** Origen del evento			
10.3.6 Identidad o nombre de los datos, componente de sistema o recursos afectados	**10.3.6** Identidad o nombre de los datos, componente de sistema o recursos afectados			
10.4 Sincronizar todos los relojes y horas de todos los sistemas críticos.	**10.4** Obtener y revisar el proceso para averiguar y divulgar la hora correcta en toda la organización. Obtener y revisar igualmente las programaciones de parámetros de sistema en una muestra de componentes de sistema. Verificar que lo siguiente está incluido en el proceso y se haya implementado lo siguiente:			
	10.4.a Verificar que se usa NTP o una tecnología similar para la sincronización de la hora.			
	10.4.b Verificar que los servidores internos no están recibiendo señales de fuentes externas. [Dos o tres			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
	servidores centrales de horario dentro de la organización reciben señales externas de la hora (directamente de un radio especial, satélites GPS u otra fuente externa, basados en la Hora Atómica Internacional y la UTC (anteriormente GMT, Hora del Meridiano de Greenwich), y colaboran entre sí para mantener la hora correcta y compartirla con otros servidores internos.			
	10.4.c Verificar que el Network Time Protocol (NTP) está operando con la versión más reciente.			
	10.4.d Verificar que se designan hosts externos específicos desde los cuales los servidores que registran la hora aceptarán las actualizaciones de la hora por NTP (para prevenir que un atacante pueda cambiar el reloj). Como opción, estas actualizaciones se pueden encriptar con una clave simétrica y se pueden crear listas de control de acceso que especifican las direcciones de Internet (IP) de las máquinas clientes que recibirán el servicio NTP (para prevenir el uso no autorizado de los servidores internos de hora). Consulte www.ntp.org para obtener más información.			
10.5 Asegurar las bitácoras de auditoría para que no se puedan alterar.	**10.5** Consultar con el administrador del sistema y examinar los permisos para verificar que las bitácoras de auditoría están seguras y que no se pueden alterar de la manera siguiente:			
10.5.1 Limitar la visualización de las bitácoras de auditoría a las personas que tengan necesidad de verlas por razones de trabajo.	**10.5.1** Verificar que solamente las personas que por necesidad de su trabajo tienen que verlos puedan ver los archivos de bitácoras de auditoría.			
10.5.2 Proteger los archivos de bitácoras de auditoría de las modificaciones no autorizadas.	**10.5.2** Verificar que los archivos de bitácoras de auditoría actuales están protegidos de las modificaciones no autorizadas mediante mecanismos de control de acceso, segregación física y/o segregación de redes.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
10.5.3 Respaldar rápidamente los archivos de bitácoras de auditoría a un servidor centralizado o medio de respaldo que sea difícil de alterar.	**10.5.3** Verificar que los archivos de bitácoras de auditoría actuales se respaldan con prontitud a un servidor de registro centralizado o medio que es difícil de alterar.			
10.5.4 Copiar los registros o bitácoras de las redes inalámbricas a un servidor de la red de acceso local (LAN).	**10.5.4** Verificar que **s**e descargan o copian los registros de las redes inalámbricas a un servidor de registro interno centralizado que es difícil de alterar.			
10.5.5 Usar software de detección para monitorear la integridad y cualquier cambio en los archivos (tales como Tripwire) en las bitácoras para asegurar que los datos existentes en dichos registros no se puedan cambiar sin generar un alerta (aunque al agregar nuevos datos no se deberá generar un alerta).	**10.5.5** Verificar el uso del monitoreo de la integridad de archivos o de un software de detección de cambios en los registros observando las programaciones de los sistemas y los archivos supervisados, así como los resultados de estas actividades de vigilancia.			
10.6 Revisar los registros y bitácoras de todos los componentes de sistemas al menos diariamente. Estas revisiones deben incluir todos los servidores que realicen funciones de seguridad como servidores IDS y de autenticación (AAA) (por ejemplo, RADIUS). *Nota: Se puede usar la cosecha de bitácoras, parsing y herramientas para generar alertas para cumplir con el Requisito 10.6,*	**10.6.a** Obtener y examinar las políticas y los procedimientos de seguridad y determinar que se incluyen procedimientos para revisar los registros de seguridad al menos una vez al día, y que se requiere el seguimiento de las excepciones.			
	10.6.b Por medio de la observación y de consultas, determinar que se realizan revisiones regulares de los registros en el caso de todos los componentes de sistema.			
10.7 Retener el historial de bitácoras de auditoría durante al menos un año, con un mínimo de tres meses de disponibilidad en línea.	**10.7.a** Obtener y examinar las políticas y los procedimientos de seguridad y verificar que los mismos incluyen políticas de retención de registros de auditoría y que dicha retención es de al menos un año.			
	10.7.b Verificar que todos los registros de auditoría están disponibles en línea o en cinta durante al menos un año.			

Requisito 11: *Probar regularmente los sistemas y procesos de seguridad.*

Los delincuentes e investigadores continuamente descubren nuevas vulnerabilidades que se introducen a través del nuevo software. Los sistemas, procesos y programas deben probarse frecuentemente para garantizar que los mismos mantengan su seguridad a través del tiempo y los cambios.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
11.1 Probar anualmente los controles de seguridad, limitaciones, conexiones de redes y restricciones para asegurar que puedan identificar o detener en forma apropiada cualquier intento de uso no autorizado. Usar un analizador inalámbrico al menos trimestralmente para identificar todos los dispositivos inalámbricos en uso.	**11.1.a** Confirmar mediante consultas con el personal de seguridad e inspección de los códigos, documentación y procesos relevantes que se hacen pruebas periódicas de seguridad de los dispositivos dentro del ambiente de datos de los tarjetahabientes.			
	11.1.b Verificar que se usa al menos trimestralmente un analizador inalámbrico para identificar todos los dispositivos inalámbricos.			
11.2 Realizar escanes de vulnerabilidad de redes internas y externas al menos trimestralmente y después de cualquier cambio significativo en la red (por ejemplo, instalación de nuevos componentes de sistemas, cambios en la topología de red, modificación de reglas de cortafuegos, mejora de productos). *Nota: Los escanes externos de vulnerabilidad trimestrales deberá realizarlos un proveedor calificado especializado en escanes de la industria de tarjetas de pago. El personal interno podrá realizar los escanes después de hacer cambios en las redes.*	**11.2.a** Inspeccionar los cuatro escanes de vulnerabilidad más recientes de las redes, hosts y aplicaciones para verificar que se hacen pruebas de seguridad periódicas de los dispositivos dentro del ambiente de datos de los tarjetahabientes. Verificar que el proceso de escaneo incluye nuevos escanes hasta que se obtenga un resultado “limpio” en todos los casos.			
	11.2.b Para verificar que se realizan escanes externos trimestralmente de acuerdo con los Procedimientos de Escaneo de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI), inspeccionar los resultados de los escanes externos de vulnerabilidad correspondientes a los últimos cuatro trimestres para verificar que: • Se realizaron cuatro escanes trimestrales en el período más reciente de 12 meses. • Los resultados de cada escán satisfacen los Procedimientos de Escaneo de Vulnerabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI) (por			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
	ejemplo, no existen vulnerabilidades urgentes, críticas ni ninguna alta vulnerabilidad). • Los escanes fueron realizados por un proveedor aprobado para realizar los Procedimientos de Escaneo de Vulnerabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI).			
11.3 Realizar pruebas de penetración de la infraestructura de la red y aplicaciones al menos una vez al año y después de actualizar o mejorar significativamente la infraestructura o cualquier aplicación (por ejemplo, actualización del sistema operativo, adición de una subred al ambiente, adición de un servidor de Web al ambiente). Estas pruebas de penetración deben incluir lo siguiente:	**11.3** Obtener y examinar los resultados de las últimas pruebas de penetración para verificar que estas pruebas de penetración se realizan como mínimo una vez al año y después de cambios significativos al ambiente. Verificar que se ha corregido cualquier vulnerabilidad detectada. Verificar que las pruebas de penetración incluyen:			
11.3.1 Pruebas de penetración de capas de red	**11.3.1** Pruebas de penetración de capas de red			
11.3.2 Pruebas de penetración de capa de aplicación	**11.3.2** Pruebas de penetración de capa de aplicación			
11.4 Usar sistemas de detección de intrusiones en la red, sistemas de detección de intrusiones basados en host y/o sistemas de prevención de intrusiones para monitorear todo el tráfico de la red y alertar al personal sobre cualquier sospecha de compromiso de seguridad. Mantener todos los motores de detección y prevención de intrusiones al día.	**11.4.a** Observar el uso del software de detección y/o prevención de intrusiones en la red. Verificar que se monitorea todo el tráfico crítico de la red en el ambiente de datos de los tarjetahabientes.			
	11.4.b Confirmar que se han implementado y existen dispositivos de detección y/o prevención de intrusiones (IDS y/o IPS) para monitorear y alertar al personal cuando se sospeche un compromiso de seguridad.			
	11.4.c Examinar las configuraciones IDS e IPS y confirmar que los dispositivos IDS/IPS se configuran, mantienen y actualizan de acuerdo con las instrucciones de cada proveedor, a fin de asegurar una protección óptima.			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECIDO	FECHA PROGRAMADA/ COMENTARIOS
11.5 Implementar software de monitoreo de la integridad de los archivos para alertar al personal sobre cualquier modificación no autorizada de un sistema o contenido de un archivo crítico y realizar comparaciones de archivos críticos al menos semanalmente. *Los archivos críticos no son necesariamente aquellos que contienen datos de los tarjetahabientes. Para fines de monitoreo de integridad de archivos, los archivos críticos son normalmente aquellos que no cambian regularmente, pero cuya modificación podría indicar un compromiso o riesgo de compromiso de seguridad del sistema. Los productos para monitorear la integridad de los archivos normalmente vienen preconfigurados con los archivos críticos para el sistema operativo relacionado. Otros archivos críticos, tales como los de aplicaciones individuales, deben ser evaluados y definidos por el comercio o proveedor de servicio.*	**11.5** Verificar el uso de los productos para proteger la integridad de los sistemas observando las programaciones de los sistemas y los archivos monitoreados, así como revisando los resultados de dichas actividades de vigilancia.			

Mantener una Política de Seguridad de la Información

Requisito 12: Mantener una política que contemple la seguridad de la información para los empleados y contratistas.

Una política sólida de seguridad establece la pauta de la seguridad en toda la compañía y hace a los empleados tomar conciencia de lo que se espera de ellos. Todos los empleados deben estar conscientes del carácter confidencial de los datos y de su responsabilidad de protegerlos.

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
12.1 Establecer, mantener y diseminar una política de seguridad que logre lo siguiente:	**12.1** Examinar la política de seguridad de la información y verificar que la misma se publica y disemina a todos los usuarios de sistemas relevantes (incluyendo vendedores, contratistas y socios comerciales).			
12.1.1 Contemple todos los requisitos de esta especificación.	**12.1.1** Verificar que la política contempla todos los requisitos de esta especificación.			
12.1.2 Incluya un proceso anual para identificar amenazas y vulnerabilidades y que traiga como resultado una evaluación formal de los riesgos.	**12.1.2** Verificar que la política de seguridad de la información incluye un proceso anual para identificar amenazas y vulnerabilidades y trae como resultado una evaluación formal de los riesgos.			
12.1.3 Incluya una revisión al menos una vez al año y una actualización cuando el ambiente cambie.	**12.1.3** Verificar que la política de seguridad de la información incluye una revisión al menos anual y se actualiza cuando es necesario para reflejar los cambios en los objetivos del negocio o ambiente de riesgo.			
12.2 Desarrollar procedimientos diarios de seguridad operativa que sean congruentes con los requisitos establecidos en esta especificación (por ejemplo, procedimientos de mantenimiento de cuentas, procedimientos de revisión de registros y bitácoras).	**12.2.a** Examinar los procedimientos operativos diarios. Verificar que son congruentes con esta especificación e incluyen procedimientos administrativos y técnicos para cada uno de los requisitos.			
12.3 Desarrollar políticas de uso de tecnologías críticas que utilizan los	**12.3** Obtener y examinar la política de uso de tecnologías críticas por parte de los empleados y verificar			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
empleados (como modems y dispositivos inalámbricos), a fin de definir el uso apropiado de estas tecnologías por parte de todos los empleados y contratistas. Asegurar que estas políticas de uso requieran lo siguiente:	que la política contiene lo siguiente:			
12.3.1 Aprobación explícita de la administración.	**12.3.1** Verificar que la política de uso requiere aprobación explícita de la administración para usar los dispositivos.			
12.3.2 Autenticación para el uso de la tecnología.	**12.3.2** Verificar que la política de uso requiere que todos los dispositivos se autentiquen con el nombre de usuario y contraseña u otro tipo de autenticación (por ejemplo, token).			
12.3.3 Una lista de todos los dispositivos y personal que tiene acceso a ellos.	**12.3.3** Verificar que la política de uso requiere una lista de todos los dispositivos y miembros del personal autorizados para usarlos.			
12.3.4 Etiquetas en los dispositivos que indiquen su dueño, información de contacto y propósito.	**12.3.4** Verificar que la política de uso requiere etiquetas en los dispositivos para indicar el dueño, la información de contacto y la finalidad del mismo.			
12.3.5 Usos aceptables de la tecnología.	**12.3.5** Verificar que la política de uso requiere usos aceptables de la tecnología,			
12.3.6 Ubicaciones aceptables en la red para estas tecnologías.	**12.3.6** Verificar que la política de uso requiere ubicaciones de red aceptables para la tecnología.			
12.3.7 Una lista de los productos aprobados por la empresa.	**12.3.7** Verificar que la política de uso requiere una lista de los productos aprobados por la empresa.			
12.3.8 Desconexión automática de las sesiones de módem después de un período específico de inactividad.	**12.3.8** Verificar que la política de uso requiere la desconexión automática de las sesiones de módem después de un determinado período de inactividad.			
12.3.9 Activación de modems por parte del proveedor solamente cuando sea necesario, con	**12.3.9** Verificar que la política de uso requiere la activación de modems utilizados por los proveedores solamente cuando es estrictamente necesario, y			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
desactivación inmediata después del uso.	desactivación inmediata después del uso.			
12.3.10 Al acceder a los datos de los tarjetahabientes en forma remota por módem, prohibir el almacenaje de dichos datos en discos duros locales, disquetes y otros medios externos. Prohibición de las funciones que permiten cortar y pegar e imprimir datos durante el acceso remoto.	**12.3.10** Verificar que la política de uso prohíbe el almacenaje de datos de los tarjetahabientes en discos duros locales, disquetes y otros medios externos al obtener acceso a dichos datos remotamente a través de un módem. Desactivar también las funciones cortar y pegar e imprimir durante el acceso remoto.			
12.4 Garantizar que la política y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información en el caso de todos los empleados y contratistas.	**12.4** Verificar que las políticas de seguridad de la información definen claramente las responsabilidades tanto de los empleados como de los contratistas de velar por la seguridad de los datos.			
12.5 Asignar a una persona o equipo las siguientes responsabilidades de administración de seguridad de la información:	**12.5** Verificar la asignación formal de la responsabilidad por la seguridad de la información a un Funcionario Jefe de Seguridad u otro funcionario de la administración con conocimientos adecuados sobre el tema. Obtener las políticas y los procedimientos de seguridad de la información para verificar que las siguientes responsabilidades se han asignado específica y formalmente:			
12.5.1 Establecer, documentar y distribuir las políticas y los procedimientos de seguridad.	**12.5.1** Verificar que la responsabilidad de crear y distribuir las políticas y los procedimientos de seguridad está formalmente asignada.			
12.5.2 Monitorear y analizar los alertas y la información de seguridad y distribuirlos al personal apropiado.	**12.5.2** Verificar que la responsabilidad de monitorear y analizar los alertas de seguridad y distribuir la información al personal de administración de las unidades de seguridad y negocio apropiadas está formalmente asignada.			
12.5.3 Establecer, documentar y distribuir procedimientos de respuesta	**12.5.3** Verificar que la responsabilidad de crear y distribuir los procedimientos de respuesta a incidentes de seguridad y procedimientos para elevar el caso a			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
a incidentes y procedimientos para acudir a una autoridad superior a fin de asegurar un manejo oportuno y eficaz en todas las situaciones.	una autoridad superior está formalmente asignada.			
12.5.4 Administrar las cuentas de usuarios incluyendo la adición, eliminación y modificación de información.	**12.5.4** Verificar que la responsabilidad de administrar las cuentas de los usuarios y la autenticación está formalmente asignada.			
12.5.5 Monitorear y controlar todo el acceso a los datos.	**12.5.5** Verificar que la responsabilidad de monitorear y controlar todos los accesos a los datos está formalmente asignada.			
12.6 Implementar un programa formal de información sobre la seguridad para que todos los empleados estén conscientes de la importancia de la seguridad de los datos:	**12.6.a** Verificar la existencia de un programa formal de información sobre la seguridad para todos los empleados.			
	12.6.b Obtener y examinar la documentación del programa para crear conciencia sobre la seguridad y hacer lo siguiente:			
12.6.1 Educar a los empleados al contratarlos y al menos anualmente (por ejemplo, por medio de afiches, cartas, memorandos, reuniones y promociones).	**12.6.1.a** Verificar que el programa de información sobre la seguridad brinda múltiples métodos para comunicar y educar a los empleados sobre este tema (afiches, cartas, reuniones, etc.)			
	12.6.1.b Verificar que los empleados asisten a las sesiones de capacitación al ser contratados y al menos anualmente.			
12.6.2 Requerir a los empleados que hagan constar por escrito que han leído y comprendido la política y los procedimientos	**12.6.2** Verificar que el programa de información sobre la seguridad requiere que los empleados hagan constar por escrito que han leído y comprendido la política de seguridad de la información de la empresa.			
12.7 Hacer una investigación de antecedentes de los candidatos a empleo para minimizar el riesgo de ataques procedentes de fuentes internas. *En el caso de los empleados que sólo tengan acceso a un número de tarjeta*	**12.7** Consultar con la administración del departamento de Recursos Humanos y verificar que existe un proceso establecido para la averiguación de antecedentes de los posibles empleados que tendrán acceso a los sistemas, redes o datos de los tarjetahabientes. Estas verificaciones deben incluir verificaciones previas al empleo, antecedentes penales, antecedentes de crédito y			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
en un momento dado para facilitar una transacción, tales como los cajeros en las tiendas, este requisito es solamente una recomendación.	referencias.			
12.8 Si los datos de los tarjetahabientes se comparten con proveedores de servicio, requerir contractualmente lo siguiente:	**12.8** Si la entidad auditada comparte los datos de los tarjetahabientes con otra compañía, obtener y examinar los contratos entre la organización y los terceros que manejen datos de los tarjetahabientes (por ejemplo, instalaciones donde se guardan cintas, proveedores de servicios administrados como compañías de hospedaje de Web o proveedores de servicios de seguridad, o aquellos que reciben datos para fines de modelación de patrones y tendencias de fraude). Hacer lo siguiente:			
12.8.1 Los proveedores de servicio deben adherirse a los Requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI).	**12.8.1** Verificar que el contrato contiene disposiciones que requieren la adherencia a los requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.			
12.8.2 Acuerdo que incluye un reconocimiento al efecto de que el proveedor de servicio es responsable por la seguridad de los datos de los tarjetahabientes que tiene en su posesión.	**12.8.2** Verificar que el contrato contiene disposiciones relativas a la obligación del tercero de reconocer su responsabilidad por mantener en forma segura los datos de los tarjetahabientes.			
12.9 Implementar un plan de respuesta en caso de incidente. Estar preparado para responder inmediatamente a una violación del sistema.	**12.9** Obtener y examinar el Plan de Respuesta a Incidentes y los procedimientos relacionados y hacer lo siguiente:			
12.9.1 Crear un plan de respuesta a incidentes, el cual se usará en caso de un compromiso de la seguridad del sistema. Asegurar que el plan contemple, como mínimo, procedimientos específicos de respuesta a incidentes,	**12.9.1.** Verificar que el Plan de Respuesta a Incidentes y los procedimientos relacionados incluyen: • Roles, responsabilidades y estrategias de comunicación en caso de ocurrir un compromiso de seguridad • Cobertura y respuestas para todos los componentes de sistemas críticos			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
recuperación comercial y reanudación de actividades comerciales, procesos de respaldo de datos, roles y responsabilidades y estrategias de comunicación y contacto (por ejemplo, informar a los Adquirentes y a las asociaciones de tarjetas de pago).	• Notificación, como mínimo, a las asociaciones de tarjetas de crédito y Adquirentes • Estrategia para la continuación del negocio después del compromiso de seguridad • Referencia o inclusión de los procedimientos de respuesta a incidentes de las asociaciones de tarjetas • Análisis de los requisitos legales para reportar los compromisos de seguridad (por ejemplo, según la ley 1386 de California, se requiere a cualquier negocio que incluya a residentes de California en su base de datos notificar a los consumidores afectados en caso de sospecharse o de ocurrir un compromiso de seguridad).			
12.9.2 Probar el plan al menos anualmente.	**12.9.2** Verificar que el plan se prueba al menos anualmente.			
12.9.3 Designar a miembros específicos del personal que estén disponibles 24 horas al día los 7 días de la semana para responder a los alertas.	**12.9.3** Verificar por medio de la observación y la revisión de las políticas que existe una cobertura de monitoreo y respuesta a incidentes durante las 24 horas del día, los 7 días de la semana, destinada a detectar cualquier señal de actividad no autorizada, alerta crítico de IDS y/o reportes de cambios no autorizados en sistemas o en el contenido de archivos críticos.			
12.9.4 Proporcionar capacitación apropiada al personal que tenga la responsabilidad de responder a una violación de la seguridad.	**12.9.4** Verificar por medio de la observación y la revisión de las políticas que se brinda capacitación en forma periódica al personal que tiene responsabilidades relacionadas con la violación de la seguridad.			
12.9.5 Incluir alertas de los sistemas de detección de intrusiones, prevención de intrusiones y monitoreo de la integridad de los archivos.	**12.9.5** Verificar por medio de la observación y revisión que los procesos de monitoreo y la respuesta a los alertas de los sistemas de seguridad están incluidas en el Plan de Respuesta a Incidentes.			
12.9.6 Contar con un proceso para modificar y mejorar el plan de respuesta a incidentes según las lecciones aprendidas de la	**12.9.6** Verificar por medio de la observación y la revisión de las políticas que existe un proceso para modificar y adaptar el plan de respuesta a incidentes de acuerdo con las lecciones aprendidas y para incorporar los desarrollos			

REQUISITOS DE LAS NORMAS DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDOS	NO ESTABLECIDOS	FECHA PROGRAMADA/ COMENTARIOS
experiencia e incorporar los desarrollos en la industria.	de la industria.			
12.10 Todos los procesadores y proveedores de servicio deben mantener e implementar políticas y procedimientos para la gestión de las entidades conectadas, los cuales incluirán lo siguiente:	**12.10** Verificar por medio de la observación, la revisión de las políticas y los procedimientos y la revisión de la documentación de apoyo que existe un proceso establecido para la gestión de las entidades conectadas realizando lo siguiente:			
12.10.1 Mantener una lista de las entidades conectadas.	**12.10.1** Verificar que se mantiene una lista de las entidades conectadas.			
12.10.2 Asegurar la debida diligencia antes de conectar a una entidad.	**12.10.2** Verificar que los procedimientos aseguran la debida diligencia antes de conectar a una entidad.			
12.10.3 Asegurar que la entidad cumple con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.	**12.10.3** Verificar que los procedimientos aseguran que la entidad cumple con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.			
12.10.4 Conectar y desconectar a las entidades siguiendo un proceso establecido.	**12.10.4** Verificar que se conecta y desconecta a las entidades siguiendo un proceso establecido.			

Apéndice A: Aplicabilidad de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para Proveedores de Servicios de Hospedaje en Redes (con Procedimientos de Prueba)

Requisito A.1: El proveedor del servicio de hospedaje en redes protegerá el ambiente de datos de los tarjetahabientes.

Según se menciona en el Requisito 12.8, se requiere que todos los proveedores de servicio que tengan acceso a los datos de los tarjetahabientes (incluidos los proveedores de servicios de hospedaje en redes) se adhieran a los requisitos establecidos en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Además, el Requisito 2.4 estipula que todos los proveedores de servicios de hospedaje en redes deberán proteger el ambiente y los datos hospedados de cada entidad. Por consiguiente, los proveedores de servicios de hospedaje en redes deberán dar especial consideración a lo siguiente:

Requisitos	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECISO	FECHA PROGRAMADA/COMENTARIOS
A.1 Proteger el ambiente y los datos hospedados de cada entidad (es decir, del comercio, del proveedor de servicio o de otra entidad) según se indica en los puntos A.1.1 a A.1.4: El proveedor de servicios de hospedaje en redes deberá cumplir con estos requisitos, así como con otras secciones relevantes de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). *Nota: Aunque el proveedor del servicio de hospedaje cumpla con estos requisitos, el cumplimiento de*	**A.1** Específicamente en el caso de la auditoría de cumplimiento con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI) de un **Proveedor de Hospedaje Compartido**, verificar que dicho **Proveedor de Hospedaje Compartido** protegen el ambiente y los datos hospedados, seleccionar una muestra de servidores (Microsoft Windows y Unix/Linux) a través de una muestra representativa de comercios y proveedores de servicio, y verificar los requisitos **A.1.1** al **A.1.4** a continuación.			

Requisitos	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECISO	FECHA PROGRAMADA/COMENTARIOS
la entidad que utiliza los servicios de hospedaje de dicho proveedor no está necesariamente garantizado. Cada entidad deberá cumplir individualmente con las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y validar su cumplimiento en la forma que sea aplicable.				
A.1.1 Asegurar que cada entidad tenga acceso únicamente a su propio ambiente de datos de tarjetahabientes.	**A.1.1** Si un proveedor de servicio de hospedaje compartido (por ejemplo, comercios y proveedores de servicio) permite a las entidades ejecutar sus propias aplicaciones, verificar que los procesos de dichas aplicaciones se ejecutan utilizando una ID única de la entidad. Por ejemplo: • Ninguna entidad en el sistema puede usar una ID de usuario de un servidor de Web compartida. • Todos los archivos de comandos CGI (scripts) de una entidad deben crearse y ejecutarse como ID de usuario única de dicha entidad.			
A.1.2 Restringir el acceso y los privilegios de cada entidad solamente a su propio ambiente de datos de tarjetahabientes.	**A.1.2.a** Verificar que la ID de usuario de cualquier proceso de aplicación no corresponde a un usuario privilegiado (root/administrativo).			

Requisitos	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECISO	FECHA PROGRAMADA/COMENTARIOS
	A.1.2.b Verificar que cada entidad (comercio, proveedor de servicio) tiene permiso para leer, escribir y ejecutar únicamente aquellos archivos y directorios de su propiedad o para los archivos de sistema necesarios (restringidos por medio de permisos de archivos de sistema, listas de control de accesos, chroot, jailshell, etc.). IMPORTANTE: Está prohibido compartir los archivos de una entidad con un grupo.			
	A.1.2.c Verificar que los usuarios de una entidad no tienen acceso de escritura a archivos binarios de sistema compartidos.			
	A.1.2.d Verificar que solamente la entidad que es propietaria de las mismas puede ver las entradas en las bitácoras y que el acceso está restringido a dicha entidad.			
	A.1.2.e A fin de asegurar que ninguna entidad pueda monopolizar los recursos de servidores para explotar vulnerabilidades (error, carrera y condiciones de reinicio que resulten, por ejemplo, en overflows de los buffers), verificar que hay restricciones implementadas para el uso de estos recursos de sistema: • Espacio de disco • Ancho de banda • Memoria • Unidad central de computación (CPU)			
A.1.3 Asegurar que estén habilitadas las bitácoras de auditoría y que sean únicas para el ambiente de datos de tarjetahabientes de cada entidad y cumplan con el Requisito 10 de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago.	**A.1.3.a** Verificar que el proveedor de servicio de hospedaje compartido ha habilitado las bitácoras y el registro en las mismas para cada ambiente hospedado de comercio y proveedor de servicio y que: • Se han habilitado bitácoras para aplicaciones comunes de terceros. • Las bitácoras están activas por parámetro automático del sistema. • Las bitácoras están disponibles para la revisión por			

Requisitos	PROCEDIMIENTOS DE PRUEBA	ESTABLECIDO	NO ESTABLECISO	FECHA PROGRAMADA/COMENTARIOS
	parte de la entidad propietaria. • La ubicación de las bitácoras se comunica claramente a la entidad propietaria.			
A.1.4 Habilitar procesos que aseguren la investigación forense oportuna en caso de un compromiso de la seguridad de cualquier comercio hospedado o proveedor de servicios.	**A.1.4** Verificar que el proveedor de hospedaje compartido cuenta con políticas documentadas que disponen una investigación forense de los servidores relacionados en caso de un compromiso de seguridad.			

Apéndice B – Controles Compensatorios

Controles Compensatorios – General

Podrían considerarse controles compensatorios para la mayoría de los requisitos de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) cuando una entidad no pueda cumplir con una especificación técnica de un requisito pero tenga suficientemente mitigado el riesgo asociado con la misma. Véase el Glosario de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago para obtener una definición completa de los controles compensatorios.

La eficacia de un control compensatorio depende de las características específicas del ambiente en el cual se implementa el control, los controles de seguridad que lo rodeen y la configuración del control. Las empresas deben estar conscientes de que un control compensatorio en particular no será eficaz en todos los ambientes. Cada control compensatorio deberá evaluarse en forma exhaustiva después de su implementación para garantizar su eficacia. Las siguientes directrices proporcionan controles compensatorios cuando las compañías no pueden lograr que los datos de los tarjetahabientes sean ilegibles de conformidad con el requisito 3.4.

Controles Compensatorios para el Requisito 3.4

En el caso de las empresas que no puedan lograr que los datos de los tarjetahabientes sean ilegibles (por ejemplo, por encriptación) debido a restricciones técnicas o limitaciones comerciales, podrían considerarse controles compensatorios. *Únicamente las compañías que hayan pasado por un análisis de riesgo y tengan restricciones tecnológicas o comerciales documentadas y legítimas pueden considerar el uso de controles compensatorios para cumplir con los requisitos.*

Las empresas que consideren controles compensatorios para hacer ilegibles los datos de los tarjetahabientes deben estar conscientes del riesgo que corren al mantener estos datos en forma legible. Generalmente los controles deben proporcionar protección adicional para mitigar cualquier riesgo adicional que corran los datos legibles de los tarjetahabientes. Los controles considerados deberán ser adicionales a los controles requeridos en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y deben satisfacer la definición de “Controles Compensatorios” que se da en el Glosario de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Los controles compensatorios pueden consistir en un dispositivo o conjunto de dispositivos, aplicaciones y controles que cumplan con **todas** las condiciones siguientes:

1. Proporcionar segmentación/abstracción adicional (por ejemplo, a nivel de capa de red).

2. Proporcionar la capacidad de restringir el acceso a los datos de los tarjetahabientes o bases de datos basándose en los siguientes criterios:

- Dirección IP /dirección Mac
- Aplicación/servicio
- Cuentas/grupos de usuarios
- Tipo de datos (filtrado de paquete)

3. Restringir el acceso lógico a la base de datos.
    - Controlar el acceso lógico a la base de datos en forma independiente al Directorio Activo o Lightweight Directory Access Protocol (LDAP).
4. Prevenir/detectar ataques comunes a las aplicaciones o bases de datos (por ejemplo, inyección de SQL).

Apéndice C: Hoja de Trabajo de Controles Compensatorios/ Ejemplo Completado

Ejemplo

1. Restricciones: Listar restricciones que impiden cumplir con el requisito original.

   La Compañía XYZ emplea Servidores Unix independientes sin LDAP. Como tal, cada servidor requiere un procedimiento de inicio de conexión (login) “root”. No es posible para la Compañía XYZ gestionar la conexión “root” ni tampoco es factible registrar en una bitácora toda la actividad “root” de cada usuario.

2. Objetivo: Definir los objetivos del control original; identificar el objetivo que cumple el control compensatorio.

   El objetivo de requerir un procedimiento único e individual de inicio de conexión es dual. En primer lugar, no se considera aceptable desde una perspectiva de seguridad compartir las credenciales de conexión. En segundo lugar compartir la conexión imposibilita declarar en forma definitiva que una persona es responsable por una acción en particular.

3. Riesgo Identificado: Identificar cualquier riesgo adicional que plantea la falta del control original.

   El riesgo adicional se introduce al sistema de control de accesos al no asegurar que todos los usuarios tengan una ID única y sea posible rastrearlos.

4. Definición de Controles Compensatorios: Definir los controles compensatorios y explicar cómo cumplen los objetivos del control original y el riesgo incremental, de haberlo.

   La Compañía XYZ va a requerir que todos los usuarios realicen el procedimiento de conexión con los servidores desde su computador de mesa utilizando el comando SU. SU permite a un usuario acceder a la cuenta “root” y realizar acciones bajo la cuenta “root”, pero el acceso se puede registrar en el directorio su-log. De esta manera es posible rastrear las acciones de cada usuario por medio de la cuenta SU.