



PCI DSS y Productos de Seguridad de Red GFI

Requerimientos PCI DSS	ESM 7	LANSS 8
Requerimiento 1: Instalar y mantener un cortafuegos para proteger la información de titulares de tarjetas		
1.3 Crear una configuración de cortafuegos para restringir las conexiones a la información de titulares de tarjetas		
1.3.1 Restringir el tráfico entrante de Internet a las direcciones IP de la DMZ	●	
1.3.6 Asegurar y sincronizar los archivos de configuración de enrutadores	●	
1.3.7 Denegar todo el resto del tráfico entrante y saliente no permitido específicamente	●	
1.3.9 Instalar software cortafuegos comercial en equipos portátiles o propiedad de los empleados con conectividad directa a Internet, utilizada para acceder a la red de la organización.		✓
Requerimiento 2: No utilizar las contraseñas por defecto suministradas por los fabricantes		
2.1 Cambiar siempre las predeterminadas suministradas por el fabricante antes de instalar un sistema en la red		●
2.2 Desarrollar estándares de configuración para todos los componentes del sistema		
2.2.2 Deshabilitar todos los servicios y protocolos innecesarios e inseguros	●	●
2.2.3 Configurar parámetros de seguridad del sistema para prevenir abusos		●
2.2.4 Eliminar todas las funcionalidades innecesarias, como scripts, drivers, servidores web		●
Requerimiento 3: Proteger la información almacenada de titulares de tarjetas		
3.5 Proteger las claves usadas para encriptar la información de titulares de tarjeta del descubrimiento o abuso		
3.5.1 Restringir el acceso a claves al menor número de custodios necesarios	●	
3.6 Documentar e implementar todos los procesos y procedimientos de gestión de las claves utilizadas para la encriptación de la información de titulares de tarjetas		
3.6.3 Almacenamiento seguro de claves	●	
Requerimiento 5: Utilizar y actualizar regularmente el software o las aplicaciones anti-virus		
5.1 Implantar software anti-virus en todos los sistemas comúnmente afectados por virus		✓
5.2 Asegurar que todos los mecanismos anti-virus están en curso y funcionando activamente		✓
Requerimiento 6: Desarrollar y mantener sistemas y aplicaciones seguros		
6.1 Asegurar que todos los componentes del sistema tienen los últimos parches de seguridad emitidos por los fabricantes		✓
6.2 Establecer un proceso para identificar vulnerabilidades de seguridad recientemente descubiertas		✓
6.4 Seguir procedimientos de control de cambios para todos los cambios de configuración de sistemas y software		
6.4.3 Probar la funcionalidad operativa		✓
6.5 Desarrollar todas las aplicaciones web en base a guías maestras de codificación segura		●
6.6 Asegurar que todas las aplicaciones web están protegidas contra ataques conocidos instalando un cortafuegos para la capa de aplicación		✓
Requerimiento 7: Restringir el acceso a la información de titulares de tarjetas según la necesidad-de-saber		
7.1 Limitar el acceso a los recursos informáticos y a la información de titulares de tarjetas sólo a aquellos cuyo trabajo requiere de dicho acceso	●	
7.2 Establecer un mecanismo para sistemas con múltiples usuarios que limite el acceso en base a la necesidad de conocimiento del usuario, y situarla en "denegar todo" salvo que se indique expresamente	●	
Requerimiento 8: Asignar un ID único a cada persona con acceso a ordenadores		
8.2 Asignar identificadores y contraseñas únicas		●
8.5 Asegurar la apropiada autenticación y gestión de contraseñas de usuarios no consumidores y administradores		
8.5.1 Controlar la adición, supresión o cambio de IDs de usuarios, credenciales y otros objetos de identificación	●	
8.5.2 Verificar la identidad del usuario antes de realizar reinicios de contraseña	●	
8.5.3 Situar la primera contraseña a un valor único por usuario y cambiarla al momento tras el primer uso	●	●
8.5.4 Revocar inmediatamente el acceso a cualquier usuario despedido	●	
8.5.5 Eliminar las cuentas de usuario inactivas al menos cada 90 días	●	●
8.5.6 Habilitar cuentas usadas por los fabricantes para la gestión remota sólo durante el tiempo necesario	●	●

Requerimientos PCI DSS	ESM 7	LANSS 8
8.5.9 Cambiar las contraseñas de usuario al menos cada 90 días		●
8.5.10 Requerir una longitud mínima de contraseña de al menos siete caracteres		●
8.5.13 Limitar los intentos repetidos de acceso bloqueando el ID de usuario tras no más de seis intentos	●	
8.5.16 Autenticar todo acceso a cualquier base de datos que contenga información de titulares de tarjetas	●	
Requerimiento 10: Rastrear y monitorizar todo acceso a los recursos de red y a la información de titulares de tarjetas		
10.1 Registrar todos los accesos de usuarios a componentes del sistema, especialmente de los usuarios administrativos	●	
10.2 Implementar auto rastreos de auditoría en todos los sistemas para rastrear los siguientes sucesos:		
10.2.1 Todos los accesos individuales a la información de titulares de tarjetas	●	
10.2.2 Todas las acciones llevadas a cabo por cualquier individuo con privilegios raíz o administrativos	✓	
10.2.3 Acceso a todos los rastreos de auditoría	✓	
10.2.4 Intentos no válidos de acceso lógico	✓	
10.2.5 Uso de mecanismos de identificación y autenticación	✓	
10.2.6 Inicialización de los registros de auditoría	✓	
10.2.7 Creación y eliminación de objetos a nivel de sistema	✓	
10.3 Registro de datos de rastreo de auditoría para todos los componentes del sistema relacionados con sucesos	✓	
10.4 Sincronizar todos los relojes y horas de sistemas críticos	●	●
10.5 Asegurar los rastros de auditoría de forma que no puedan ser alterados		
10.5.1 Limitar la revisión de rastros de auditoría a aquellos con necesidad laboral	●	
10.5.2 Proteger los archivos de rastros de auditoría de modificaciones no autorizadas	●	
10.5.5 Utilizar software de control de integridad y cambios en archivos de registro para asegurar que la información de los registros no pueda ser cambiada (excepto por nuevos datos) sin generación de alertas.	✓	
10.6 Revisar los registros de todos los componentes del sistema al menos diariamente	✓	
Requerimiento 11: Testear regularmente la seguridad de los sistemas y procesos		
11.1 Probar los controles de seguridad, limitaciones, conexiones de red y restricciones anualmentepara asegurar la capacidad de identificar y detener adecuadamente cualquier intento de acceso no autorizado	●	✓
11.2 Ejecutar escaneos internos y externos de vulnerabilidad de red al menos trimestralmente		✓
11.4 Utilizar sistemas de detección de intrusos en la red, sistemas de detección de intrusos basado en host, y sistemas de prevención de intrusos para monitorizar y avisar al personal de compromisos sospechosos	●	●
11.5 Implantar software de monitorización de integridad de archivos para alertar al personal de la modificación no autorizada de sistemas críticos o de contenido de archivos	✓	✓

Leyenda

✓ Requerimiento completamente soportado

● Requerimiento parcialmente soportado mediante adaptación de informes o producto. Se pueden aplicar condiciones.

NOTA: Las condiciones aplicables incluyen, pero no se limitan a:

- Opciones de Seguridad Windows, tales como Directiva de Contraseñas y Directiva de Auditoría
- Opciones de cuentas de usuario
- Que el software y los dispositivos de terceros, como los cortafuegos, estén apropiadamente instalados y configurados

