



PCI DSS y GFI EventsManager 7

Requerimientos PCI DSS	Auditoría	Monitorización y Generación de informes	Alertas	Hacer cumplir	Observaciones
Requerimiento 1: Instalar y mantener un cortafuegos para proteger la información de titulares de tarjetas					
1.3 Creación 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		●	●		Crear nuevas reglas
1.3.6 Asegurar y sincronizar los archivos de configuración de enrutadores		✓	✓		Personalizar reglas e informes predefinidos **
1.3.7 Denegar todo el resto del tráfico entrante y saliente no permitido específicamente		●	●		Crear nuevas reglas
Requerimiento 2: No utilizar las contraseñas por defecto suministradas por los fabricantes					
2.2 Desarrollar estándares de configuración para todos los componentes del sistema					
2.2.2 Deshabilitar todos los servicios y protocolos innecesarios e inseguros		●	●		Requerimiento no soportado por defecto *
Requerimiento 3: Proteger la información almacenada de titulares de tarjetas					
3.5 Proteger las claves que codifican la información de titulares de tarjeta del descubrimiento o abuso:					
3.5.1 Restringir el acceso a claves al menor número de custodios necesarios		✓	✓		Personalizar reglas e informes predefinidos **
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		✓	✓		Personalizar reglas e informes predefinidos **
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		✓	✓		Personalizar reglas e informes predefinidos **
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 específicamente		✓	✓		Personalizar reglas e informes predefinidos **
Requerimiento 8: Asignar un ID único a cada persona con acceso a ordenadores					
8.5 Asegurar la apropiada autenticación de usuario y gestión de contraseñas para usuarios no consumidores y administradores					
8.5.1 Controlar la adición, eliminación o modificación de IDs de usuarios, credenciales y otros objetos de identificación		✓	✓		Reglas e informes predefinidos
8.5.2 Verificar la identidad del usuario antes de realizar reinicios de contraseña		✓	✓		Reglas e informes predefinidos
8.5.3 Situar la primera contraseña a un valor único por usuario y cambiarla tras el primer uso		✓			Informes predefinidos
8.5.4 Revocar inmediatamente el acceso a cualquier usuario despedido		✓	✓		Reglas e informes predefinidos
8.5.5 Eliminar las cuentas de usuario inactivas al menos cada 90 días		✓			Informes predefinidos
8.5.6 Habilitar cuentas para la gestión remota de los fabricantes sólo el tiempo necesario		✓	✓		Reglas e informes predefinidos

Requerimientos PCI DSS	Auditoría	Monitorización y Generación de informes	Alertas	Hacer cumplir	Observaciones
8.5.13 Limitar los intentos repetidos de acceso bloqueando el ID de usuario tras no más de seis intentos		✓			Informes predefinidos
8.5.16 Autenticar todo acceso a cualquier base de datos con información de titulares de tarjetas		✓	✓		Reglas e informes predefinidos
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 a componentes del sistema, máxime de los usuarios administrativos	✓	✓			Personalizar reglas e informes predefinidos **
10.2 Implementar auto rastreos de auditoría en todos los sistemas para reconstruir los siguientes sucesos:					
10.2.1 Todos los accesos individuales a la información de titulares de tarjetas	✓	✓		✓	Personalizar reglas e informes predefinidos **
10.2.2 Todas las acciones llevadas a cabo por cualquier individuo con privilegios raíz o administrativos	✓	✓		✓	Reglas predefinidas
10.2.3 Acceso a todos los rastreos de auditoría	✓	✓		✓	Reglas e informes predefinidos
10.2.4 Intentos no válidos de acceso lógico	✓	✓		✓	Reglas e informes predefinidos
10.2.5 Uso de mecanismos de identificación y autenticación	✓	✓		✓	Reglas e informes predefinidos
10.2.6 Inicialización de los registros de auditoría	✓	✓		✓	Reglas e informes predefinidos
10.2.7 Creación y eliminación de objetos a nivel de sistema	✓	✓		✓	Reglas e informes predefinidos
10.3 Registro de datos para auditoría de todos los componentes del sistema relacionados con sucesos	✓			✓	
10.4 Sincronizar todos los relojes y horas de sistemas críticos		✓	✓		Reglas predefinidas
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		✓	✓		Reglas e informes predefinidos
10.5.2 Proteger los archivos de rastros de autoría de modificaciones no autorizadas		✓	✓		Reglas e informes predefinidos
10.5.5 Usar software de control de integridad y cambios en archivos de registro para asegurar que la información no pueda ser cambiada (excepto por nuevos datos) sin generación de alertas.		✓	✓	✓	Reglas e informes predefinidos
10.6 Revisar los registros de todos los componentes del sistema al menos diariamente		✓		✓	Programar informes predeterminados
Requerimiento 11: Testear regularmente la seguridad de los sistemas y procesos					
11.1 Probar los controles de seguridad, limitaciones, conexiones de red y restricciones anualmente para asegurar la capacidad de identificar y detener adecuadamente cualquier intento de acceso no autorizado		●	●		
11.4 Utilizar sistemas de detección de intrusos en red, sistemas de detección de intrusos en host, y sistemas de prevención de intrusos para monitorizar y avisar al personal de actividades sospechosas		●	●	●	Crear nuevas reglas
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			✓	✓	Reglas e informes predefinidos

* Se necesita la creación de una nueva regla de procesamiento de sucesos que no pueda forzar directamente este requerimiento pero apoye a los administradores mediante monitorización y generación de informes y alertas.

** Se necesita cambiar las opciones de configuración de las reglas e informes por defecto, mediante la especificación de parámetros consistentes con su entorno de red.

Leyenda

✓ Requerimiento completamente soportado

● Requerimiento parcialmente soportado mediante personalización de informes o del producto. Se pueden aplicar ciertas 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