

**METODOLOGIA PARA LA REVISIÓN**

**DE REGLAS DE FIREWALL**

**SIGCMA-SGSI**

Versión 2.

Agosto 2022

**Historial del Documento**

|  |  |  |  |
| --- | --- | --- | --- |
| Versión | Fecha | Comentarios | Por |
| 1 | 28-07-2022 | Versión Inicial | GPET |
| 2 | 29-09-2022 | Vesión revisada con acciones de mejora | GPET |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contenido

[OBJETIVO 4](#_Toc110434071)

[GLOSARIO 4](#_Toc110434072)

[1. METODOLOGÍA PARA LA REVISIÓN DE REGLAS DE FIREWALL 5](#_Toc110434073)

[1.1. Paso 1: Revise el diagrama de red 5](#_Toc110434074)

[1.2. Paso 2: Revise los diagramas de flujo de información 6](#_Toc110434075)

[1.3. Paso 3: Revisión de la configuración del firewall 6](#_Toc110434076)

[**1.3.1.** **Verifique la configuración estándar** 6](#_Toc110434077)

[**1.3.2.** **Evaluar la configuración actual del firewall** 9](#_Toc110434078)

[1.4. Paso 4: Revisión del conjunto de reglas de firewall 9](#_Toc110434079)

[**1.4.1.** **Análisis de tráfico** 9](#_Toc110434080)

[**1.4.2.** **Análisis de rendimiento** 10](#_Toc110434081)

[**1.4.3.** **Prepare la actualización del conjunto de reglas de firewall** 10](#_Toc110434082)

[1.5. Paso 5: consolidar los hallazgos 11](#_Toc110434083)

[1.6. Paso 6: Remediación de deficiencias 11](#_Toc110434084)

[1.7. Paso 7: Presente el informe final a la alta gerencia 12](#_Toc110434085)

[1.8. Paso 8: Actualice los logs de auditoría de revisión del firewall 14](#_Toc110434086)

[2. MANTENIMIENTO DEL CUMPLIMIENTO DEL CONJUNTO DE REGLAS DEL FIREWALL 14](#_Toc110434087)

[2.1. Revisión periódica del firewall 14](#_Toc110434088)

[2.2. Proceso de gestión de cambios 14](#_Toc110434089)

[2.3. Lista de verificación de nuevos dispositivo o aplicaciones 15](#_Toc110434090)

[2.4. Lista de verificación para dispositivos o aplicaciones fuera de servicio 16](#_Toc110434091)

[2.5. Gestión de vulnerabilidades 16](#_Toc110434092)

[2.6. Mejora continua 17](#_Toc110434093)

# OBJETIVO

Definir los pasos a seguir para evaluar la eficacia de la configuración de las reglas de los firewalls presentes en la infraestructura de la Rama Judicial e identificar oportunidades de mejora acorde con lo recomendado en las buenas prácticas internacionales.

# GLOSARIO

Para otros términos y definiciones, consultar el documento “GLOSARIO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES”

* **Firewall:** Un firewall, también conocido como cortafuegos, es un elemento informático que trata de bloquear el acceso, a una red privada conectada a Internet, a usuarios no autorizados.
* **Conexión:** Las conexiones de red son las interconexiones que se realizan para acceder al servicio de internet, que hoy día es una de las herramientas más importantes.
* **Servicio de red:** Son configurados en redes locales para mantener la seguridad y la operación amigable de los recursos. También ayudan a la red local a funcionar sin problemas y eficientemente. Los más conocidos son: DNS, DHCP, SNMP, FTP, etc.
* **Servicio inseguro:** Los servicios de red inseguros son los servicios que requieren nombres de usuario y contraseñas sin cifrar. Por ejemplo, Telnet y FTP son dos de esos servicios.
* **VPN:** Una VPN o Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local.

# METODOLOGÍA PARA LA REVISIÓN DE REGLAS DE FIREWALL

El propósito de la revisión es garantizar que la configuración del firewall y el conjunto de reglas cumplan con los requisitos de la Rama Judicial y de cumplimiento, a las buenas prácticas internacionales. A continuación, se presentan los pasos recomendados para esta revisión[[1]](#footnote-1):

1. Revisar el diagrama de red.
2. Revisar flujos de información.
3. Revise la lista de servicios, protocolos y puertos aprobados.
4. Revisar la configuración del firewall.
5. Revise el conjunto de reglas del firewall.
6. Implementar la remediación según sea necesario.
7. Preparar un informe sobre los hallazgos.
8. Actualizar la pista de auditoría de revisión del firewall.

## Paso 1: Revise el diagrama de red

* Realice un escaneo de dispositivos para descubrir todos los dispositivos en la infraestructura.
* Use los resultados de escaneo del dispositivo para verificar que el diagrama de red esté actualizado y completo.
* Si se encuentran dispositivos que no están en el diagrama de red o hay dispositivos en el diagrama de red que no fueron encontrados por el escaneo, entonces revise las solicitudes de cambio para determinar si hay una solicitud de cambio aprobada que respalde el cambio.
* Asegúrese de que cada componente en el diagrama de red esté correctamente etiquetado con su nombre de host y dirección (es) IP.

A continuación, se presentan deficiencias que se pueden presentar y las respectivas tareas de remediación asociadas:

| **Deficiencia** | **Remediación** | **Estado** |
| --- | --- | --- |
| Nuevo dispositivo encontrado en infraestructura sin solicitud de cambio aprobada | Eliminar el dispositivo de la infraestructura. |  |
| Revisar los procedimientos de gestión de cambios. Asegurar que existan mecanismos para evitar esto (por ejemplo, todos los puertos de swicth / router deben estar deshabilitados hasta que se apruebe la solicitud de cambio para habilitarlo). |  |
| El dispositivo ya no está en la infraestructura sin una solicitud de cambio aprobada | Enviar solicitud de cambio para el desmantelamiento del dispositivo (por ejemplo, deshabilitar la supervisión). |  |
| Actualizar el diagrama de red. |  |
| El nuevo dispositivo tiene una solicitud de cambio, pero el diagrama de red no está actualizado | Revise los procesos / procedimientos de gestión de cambios y aborde las brechas. Si no hay brechas en el proceso, aborde el incumplimiento de los procesos / procedimientos de gestión de cambios. |  |
| Actualizar diagrama de red. |  |
| Dispositivo eliminado con solicitud de cambio, pero diagrama de red no actualizado | Revise los procesos / procedimientos de gestión de cambios y aborde las brechas. Si no hay brechas en el proceso, aborde el incumplimiento de los procesos / procedimientos de gestión de cambios. |  |
| Actualizar diagrama de red. |  |

## Paso 2: Revise los diagramas de flujo de información

Verifique que los flujos de información se hayan obtenido para todos los componentes identificados en el diagrama de red. Tenga en cuenta que, si se identifican deficiencias en la revisión del diagrama de red, es muy probable que existan deficiencias similares en los diagramas de flujo de información.

## Paso 3: Revisión de la configuración del firewall

Para cualquier deficiencia identificada durante la revisión de la configuración, registre la eficiencia y el estado de remediación (por ejemplo, remediación implementada o pendiente).

### **Verifique la configuración estándar**

Las buenas prácticas internacionales recomiendan que se documente la configuración para todos los componentes de la infraestructura, incluidos los firewalls, y que estén alineados con los estándares de protección aceptados por la industria. También, establece que dichos estándares deben abordar los requisitos de protección de seguridad teniendo en cuenta las vulnerabilidades de seguridad conocidas y evitando (de ser posible) las no conocidas.

Este documento hace uso de los siguientes estandares aceptados por la industria:

* El Centro para la Seguridad de Internet (CIS) ([www.cisecurity.org](http://www.cisecurity.org))
* La Organización Internacional de Normalización (ISO) ([www.iso.org](http://www.iso.org))
* SANS Institute - SysAdmin, Networking and Security Institute ([www.sans.org](http://www.sans.org))
* NIST - Instituto Nacional de Estandares de Tecnología ([www.nist.gov](http://www.nist.gov)).

Los estándares especifican la configuración mínima que se debe aplicar a todos los sistemas nuevos en la infraestructura. Además, todos los sistemas deben revisarse y actualizarse en la medida que los estándares de configuración se renueven.

La siguiente tabla enumera los elementos de configuración mínimos, que se incluirán en la configuración de firewall estándar.

| **Categoría** | **Configuración de firewall estándar** | **Comentarios** |
| --- | --- | --- |
| Versión y nivel de parche | Identifique la versión actual y el nivel de parche. | Cuando se identifica un nuevo parche o versión, se debe actualizar el estándar de configuración. Asegúrese de que todos los parches críticos se hayan aplicado al firewall. Se recomienda que los parches críticos deben aplicarse dentro de un mes después del lanzamiento por parte del proveedor. |
| Servicios activos | Enumere todos los servicios, protocolos y puertos que se deshabilitarán. | A menudo, la configuración predeterminada en los firewalls tiene servicios como TELNET, servicios web habilitado de forma predeterminada. Los servicios, protocolos y puertos permitidos en el firewall pueden ser más restrictivos que los permitidos en otros sistemas acorde con las necesidades de la Rama Judicial. |
| Divulgación de privados. Direcciones IP | Identifique la configuración de los mecanismos para evitar la divulgación de direcciones IP privadas y la información de enrutamiento. | Los mecanismos apropiados incluyen uno o más de los siguientes: traducción de direcciones de red (NAT), servidores proxy, publicidad de rutas de redes privadas y / o uso del espacio de direcciones RFC 1918 para direccionamiento interno. |
| Inspección de estado | Especificar el requisito para el uso de inspección con estado |  |
| Red de arquitectura | Especifique el requisito de un firewall en cada conexión a Internet entre cualquier zona desmilitarizada y la zona de red interna |  |
| Controles de acceso | Identifique todas las cuentas de usuario proporcionadas por el proveedor (por ejemplo, cambiar nombre de usuario, contraseña). Especifique las cadenas de comunidad SNMP que se utilizarán, los servidores SNMP pueden conectarse, deshabilite SNMP SET (es decir, SNMP configurado en solo lectura). Identifique todas las cuentas necesarias para eliminar o deshabilitar. | Las cuentas con "admin" en el nombre deben cambiarse siempre que sea posible. Identifique la configuración para la integración con el control de acceso centralizado (por ejemplo, TACACS, RADIUS). |
| Sincronización de tiempo | Identificar servidores de sincronización de hora central. | Todos los componentes de la infraestructura deben sincronizarse con la misma fuente de hora central. |
| Pistas de auditoría | Identifique la configuración de registro: registre todos los intentos de acceso. Especifique la configuración para el reenvío de datos de registro a un servidor de registro centralizado. | Es posible que también desee registrar todas las conexiones a través del firewall; de ser así, la configuración debe documentarse en la configuración estándar. |
| Otro | Identifique cualquier otra configuración de seguridad disponible, como prevención de falsificación de IP, detección de DoS, bloqueo de paquetes DNS maliciosos / mal formados | Práctica recomendada de seguridad: las funciones y los mecanismos disponibles dependen de la marca, el modelo y el IOS del firewall |

### **Evaluar la configuración actual del firewall**

* Compare la configuración actual del firewall con la configuración estándar documentada y registre los ajustes requeridos.
* Realice escaneos de puertos en cada interfaz del firewall para identificar cualquier servicio innecesario o inseguro que se ejecute en el firewall. Preste especial atención a los servicios, protocolos y puertos que se ejecutan en las interfaces de Internet. Algunos protocolos, como el ping ICMP, pueden ser aceptables en las interfaces de firewall internas, pero no en las interfaces con conexión a Internet.
* Aunque se requiere que las pruebas de penetración se realicen anualmente, como parte de la revisión de la configuración del firewall, es beneficioso ejecutar pruebas de penetración específicas para investigar el comportamiento del firewall cuando recibe paquetes mal formados y paquetes inesperados.
* Inspeccione los logs del firewall en el correlacionador de eventos y verifique la presencia de datos de registro de auditoría. Verifique que el firewall registra todos los cambios de la configuración del tiempo.
* Intente iniciar sesión en el firewall utilizando las cuentas / contraseñas proporcionadas por el proveedor (las cuentas proporcionadas por el proveedor deben figurar en la configuración estándar) con el fin de verificar que las contraseñas predeterminadas se hayan cambiado. Se recomienda el uso de soluciones de escaneo de vulnerabilidades, ya que pueden informar sobre cuentas suministradas por el proveedor con contraseñas predeterminadas.
* Revise los controles de acceso establecidos para ingresar a los servidores de seguridad y las cuentas de usuario habilitadas y que la autorización de inicio de sesión se base tanto en el principio del mínimo privilegio (negar todo) y en lo que el usuario necesite conocer de acuerdo con las funciones que realice.
* Verifique la existencia y el uso de cuentas de usuario genéricas. Por estandarización, se requiere que se usen nombres de usuario únicos, y que se asignen específicamente a un individuo, para acceder a todos los componentes de la infraestructura.

## Paso 4: Revisión del conjunto de reglas de firewall

### **Análisis de tráfico**

* Para llevar a cabo las revisiones se requiere una lista del conjunto de reglas del firewall, estadísticas de uso de cada regla y datos sobre el tráfico permitido y denegado por el firewall.
* Revise el uso de "any" en el origen, destino o puerto en la sección de "permitir reglas".
* Para cada regla de "permitir", revise el tráfico y determine qué conexiones se están estableciendo con qué y por cual puerto.
* Solo el tráfico identificado en la lista de tráfico autorizado puede pasar a través del firewall. Esto se aplica no solo al tráfico entrante sino también al tráfico saliente. El filtrado de salida a menudo se pasa por alto, pero es obligatorio.
* Identifique cualquier tráfico que utilice puertos no autorizados a través del firewall.
* Para cada instancia detectada, registre las direcciones IP de origen y destino.
* Inspeccione todo el tráfico que llegue a las reglas de "denegación". El tráfico denegado puede ser una indicación de servicios, protocolos y puertos no autorizados en la infraestructura. Preste especial atención al tráfico denegado entre la DMZ y la red interna, así como al tráfico saliente y entrante de Internet.
* Registre la IP de origen y los puertos utilizados de todo el tráfico denegado que se origina en la infraestructura.
* Identifique cualquier regla de "permitir" que no tenga comentarios. Cada regla debe tener un comentario que indique el requisito o justifique su uso. Siempre que sea posible, debe incluirse en los comentarios el número solicitud de cambio asociado a la regla.
* Deben evaluarse las reglas que nunca tienen tráfico y las reglas que "traslapan" otras reglas. Las reglas que traslapan son reglas que otorgan el mismo o similar acceso a otras reglas existentes. Las reglas que nunca tienen tráfico indican la presencia de reglas más permisivas antes o que las reglas no son necesarias y pueden eliminarse.
* Preste especial atención a todas las instancias donde se aplican reglas más permisivas antes que reglas más restrictivas.
* Finalmente, verifique que haya una regla de "negar todo" al final del conjunto de reglas.

### **Análisis de rendimiento**

* La revisión del conjunto de reglas del firewall requiere examinar los patrones de tráfico en detalle.
* Revise los recuentos de aciertos en cada regla de firewall e identifique las reglas con mayor cantidad de aciertos.
* A medida que el firewall aplica las reglas al tráfico en orden secuencial, para un rendimiento óptimo se recomienda que el conjunto de reglas se organice de modo que las reglas más utilizadas estén más arriba en la política.

### **Prepare la actualización del conjunto de reglas de firewall**

* Según los resultados de la revisión del conjunto de reglas y el análisis de rendimiento, prepare un conjunto de reglas actualizadas para aplicar al firewall. El conjunto de reglas actualizadas debe abordar todas las deficiencias identificadas en la revisión , así como, cualquier mejora de rendimiento.
* Si no se ha realizado una revisión del firewall antes, lo más probable es que la lista de tráfico autorizado de reglas ajustadas tenga deficiencias.
* El mayor desafío cuando se realiza la revisión del conjunto de reglas de firewall por primera vez es que el tráfico requerido por la Rama Judicial no se comprende completamente.
* Se recomienda llevar a cabo varias iteraciones de la revisión del conjunto de reglas del firewall para alinear con la lista de tráfico autorizado.

## Paso 5: consolidar los hallazgos

* Todos los profesionales o ejecutores de las revisiones deben enviar sus formatos de resultados de revisión de firewall completos a la unidad informática e informar a la Oficina de Seguridad de la Información, los resultados de los mismos.
* El líder de revisión del firewall es responsable de consolidar todas las deficiencias identificadas, así como las acciones correctivas y el estado de cada acción correctiva en una lista consolidada.

| **Categoría** | **Deficiencias** | **Acciones de remediación** | **Estado** |
| --- | --- | --- | --- |
| Lista de tráfico autorizado |  |  |  |
| Configuración actual del firewall |  |  |  |
| Conjunto de reglas de firewall |  |  |  |
| Diagrama de Red |  |  |  |
| Configuraciones de línea de base seguras - otros sistemas |  |  |  |

## Paso 6: Remediación de deficiencias

* + 1. **No se requiere remediación**
* Si no se requiere remediación, vaya al paso 7.
  + 1. **Preparar el plan de remediación**
* El líder de revisión del firewall es responsable de preparar el plan de remediación y supervisar las tareas de este, desde la Oficina de Seguridad de la Información junto con la Unidad Informática.
* Use la lista de tráfico autorizado para crear el plan de remediación.
* Asigne un "propietario" y determine las fechas de finalización objetivo para cada tarea.
* Un ejemplo de plan de remediación se ilustra a continuación.

| **Tarea** | **Propietario** | **Fecha límite de finalización** | **Fecha de finalización** | **Estado** |
| --- | --- | --- | --- | --- |
| Aplicar el conjunto de reglas de firewall actualizado. |  |  |  |  |
| Actualizar la lista de tráfico autorizado. |  |  |  |  |
| Actualice la configuración de línea de base segura – Otros sistemas |  |  |  |  |
| Aplicar la configuración de línea de base segura actualizada |  |  |  |  |
| Actualizar la información de diagramas de flujo. |  |  |  |  |
| Aplicar el conjunto de reglas de firewall actualizado (en caso de ser necesario). |  |  |  |  |

* + 1. **Implementar la remediación**
* Implemente todas las soluciones identificadas en el informe de hallazgos.
* Los propietarios de las tareas son responsables de la preparación de los planes de implementación del cambio, la presentación de solicitudes de cambio, la implementación del cambio, la verificación, la actualización de la documentación y la obtención de la aprobación de la documentación, cuando corresponda.
* Los propietarios de tareas también son responsables de notificar al líder de revisión del firewall cuando la tarea se haya completado. El líder de revisión del firewall es responsable de actualizar el estado de cada tarea en el plan de remediación.

## Paso 7: Presente el informe final a la alta gerencia

* + 1. **Preparar informe final**
* El informe final debe incluir:
  + la fecha en que se preparó el informe final,
  + el autor del informe,
  + a quién se debe enviar el informe,
  + el resultado final de la revisión del firewall,
  + un resumen ejecutivo,
  + los formatos de la revisión completa del firewall,
  + la lista consolidada de resultados y
  + el plan de remediación (incluido el estado de todas las actividades de remediación),
  + datos de tendencias que demuestren mejora continua. Las métricas útiles incluyen el esfuerzo requerido para completar la revisión del firewall y la cantidad de deficiencias encontradas.
* Al presentar las métricas de revisiones anteriores junto con la última revisión, la Rama Judicial puede determinar si el proceso de revisión de reglas del firewall se vuelve más eficiente con el tiempo.
* El esfuerzo requerido para completar las revisiones de firewall debería disminuir con el tiempo a medida que los procedimientos se perfeccionen y el personal gane competencia.
* El número de deficiencias que no se reducen con el tiempo es una indicación de incumplimiento continuo.
* A continuación, se presenta una plantilla para el informe final:

1. Revisión de firewall <nombre (s) de host> Informe final
2. Fecha del informe final
3. Preparado por:
4. Presentado a:
5. Estado: Cumple / no cumple
6. Resumen Ejecutivo
7. Los objetivos son:
   1. Demostrar que real = aprobado
   2. Conocimiento de la alta gerencia de áreas problemáticas (por ejemplo, tráfico denegado que indica deficiencias en configuraciones de línea de base seguras en otros sistemas en la infraestructura, brechas en los procesos / procedimientos de gestión de cambios)
8. Datos de tendencias
   * 1. **Presente el informe final a la alta gerencia**

* El líder de revisión del firewall envía el informe final a la alta gerencia y solicita una reunión para presentar los resultados.
* La presentación puede incluir estadísticas para demostrar ganancias de eficiencia en el proceso de revisión del firewall.
* Un bajo esfuerzo para ejecutar la revisión del firewall y un bajo número de deficiencias detectadas indican tanto el cumplimiento continuo como la eficiencia del proceso de revisión del firewall.

## Paso 8: Actualice los logs de auditoría de revisión del firewall

* La Rama Judicial debe proporcionar pruebas al auditor del sistema de gestión de seguridad de la información que las revisiones del firewall se realizan como mínimo cada seis meses, así mismo, deberá presentar toda la documentación correspondiente.
* Como el informe final contiene toda la información requerida para satisfacer los requisitos de la ISO 27001:2013, es suficiente con salvaguardar el informe final de cada revisión del firewall en un sitio seguro, con acceso restringido.

# MANTENIMIENTO DEL CUMPLIMIENTO DEL CONJUNTO DE REGLAS DEL FIREWALL

## Revisión periódica del firewall

* Las revisiones de firewall deben realizarse, como mínimo, cada seis meses
* Para demostrar el cumplimiento, se deben mantener pistas de auditoría (ver numeral 1.8). Mantenga todos los informes de revisión del firewall en una ubicación segura y asegúrese de que se pueda acceder a ellos cuando sea necesario (por ejemplo, cuando venga el evaluador de entes de control, auditor, etc).
* La primera vez que se realiza una revisión del firewall, la revisión es efectivamente una fase de descubrimiento para determinar qué está pasando realmente en la infraestructura. Con el conocimiento adquirido en la primera revisión del firewall y los procesos y procedimientos efectivos de gestión de cambios, las revisiones posteriores del conjunto de reglas deberían requerir un esfuerzo significativamente menor ya que se minimiza la brecha entre lo aprobado y el tráfico real permitido a través del firewall.

## Proceso de gestión de cambios

* Un proceso de gestión de cambios es necesario para garantizar que se realizan las pruebas adecuadas para verificar que estos no introducen riesgos inaceptables en la infraestructura y que la documentación se mantiene actualizada a medida que se ajusta la infraestructura. Además, es un requisito de la ISO 27001:2013 y es fundamental para garantizar el cumplimiento continuo.
* Se deben identificar procedimientos de prueba de seguridad para diferentes escenarios de cambio, por ejemplo: introducción de cambios significativos en la infraestructura, cambios en las reglas del firewall, actualización de las principales versiones de software y cambios en las configuraciones estándar.
* Se recomienda incorporar la actualización del diagrama de red en el proceso de gestión de cambios, esto asegura que el diagrama de red se mantenga actualizado en todo momento y reduce el esfuerzo requerido para la preparación de auditorías y revisiones de firewall.
* También se recomienda el uso de listas de verificación, en las que se identifiquen todas las actividades que deben completarse cuando se introducen o eliminan dispositivos / aplicaciones a la infraestructura. Dichas listas permiten el control de las actividades y ayudan a reducir los riesgos relacionados con los cambios.

## Lista de verificación de nuevos dispositivo o aplicaciones

* El aprobador de cambios debe verificar que todos los elementos de la lista de verificación se aborden en el plan de implementación antes de otorgar la aprobación para continuar.
* El cambio se considera completo solo cuando se han abordado todos los elementos de la lista de verificación.
* A continuación, se muestra una lista de verificación para un nuevo dispositivo / aplicación.

| **#** | **Actividad** | **Cumple**  **(Si /No)** |
| --- | --- | --- |
| 1. | ¿El diagrama de red se encuentra actualizado? |  |
| 2. | ¿Línea base segura fue aplicada al dispositivo? |  |
| 3. | ¿El Inventario de activos y configuración (CMDB) fue actualizado?  Direcciones IP, seriales, información del contrato de soporte, propietario, custodio, equipo de soporte, etc. |  |
| 4. | ¿Los registros fueron habilitados?, ¿Los registros están siendo enviados al correlacionador de eventos? |  |
| 5. | ¿Se determino con qué otros dispositivos o aplicaciones se comunicará el nuevo dispositivo o aplicación y por qué puertos? |  |
| 6. | Si se requieren servicios, protocolos o puertos no cifrados, ¿Se han identificado, aprobado e implementado los controles compensatorios? |  |
| 7. | ¿Se requieren cambios de reglas en el Firewall? |  |
| 8. | Si se requiere un cambio de regla, ¿Se ha actualizado y aprobado la lista de tráfico autorizado? |  |
| 9. | ¿Se está llevando a cabo el monitoreo de los nuevos dispositivos o de las aplicaciones? |  |
| 10. | ¿Se está llevando a cabo copias de seguridad regulares del dispositivo o de la aplicación? |  |
| 11. | ¿Se tienen procedimientos documentados y probados para la restauración de la copia de seguridad? |  |
| 12. | ¿Se tiene procedimientos documentados y probados para llevar a cabo la instalación de parches regulares, o actualización de firmas (cuando corresponda)? |  |
| 13. | ¿Se tiene procedimientos documentados y probados para otras actividades de mantenimiento? |  |
| 14. | ¿Se llevaron a cabo pruebas funcionales? |  |
| 15. | ¿Se llevaron a cabo pruebas de seguridad?  Análisis de vulnerabilidades, escaneo de puertos, pruebas de penetración al nuevo dispositivo o aplicación y al firewall (si se requieren cambios en el firewall) |  |

## Lista de verificación para dispositivos o aplicaciones fuera de servicio

* La aprobación del cambio debe depender de que todos los elementos de la lista de verificación se cumplan en el plan de desmantelamiento. El cambio se considera completo solo cuando se han abordado todos los elementos de la lista de verificación.
* A continuación, se presenta una lista de verificación para dispositivos o aplicaciones fuera de servicio.

| **#** | **Actividad** | **Cumple**  **(Si /No)** |
| --- | --- | --- |
| 1. | ¿El diagrama de red fue actualizado? |  |
| 2. | ¿Se actualizó la documentación del flujo de información? |  |
| 3. | ¿Se actualizo el inventario de activos y configuración (CMDB)? Se debe marcar el dispositivo o aplicación como fuera de servicio. |  |
| 4. | ¿Se actualizó el correlacionador de eventos para dejar de recopilar logs del dispositivo o aplicación fuera de servicio? |  |
| 5. | Si los servicios, protocolos o puertos utilizados por los dispositivos o aplicaciones fuera de servicio ya no son necesarios, ¿Se ha actualizado la lista de tráfico autorizado? |  |
| 6. | Si ya no se requieren servicios, protocolos o puertos, ¿se han actualizado las configuraciones de línea de base seguras?  Deshabilite los servicios, protocolos y puertos no requeridos. |  |
| 7. | ¿Se ha aplicado la configuración de línea de base segura actualizada a todos los sistemas aplicables? |  |
| 8. | ¿Se requiere cambios en las reglas de Firewall?  Elimine las entradas de reglas relacionadas con los servicios, protocolos o puertos que ya no son necesarios. |  |
| 9. | ¿El dispositivo o aplicación fue eliminado de los backups periódicos? |  |
| 10. | ¿Se llevaron a cabo pruebas de seguridad?  Escaneo de vulnerabilidades, escaneo de dispositivos, escaneo de puertos. |  |

## Gestión de vulnerabilidades

* La organización debe garantizar que existan procesos y procedimientos para identificar las vulnerabilidades relacionadas con los firewalls.
* Las advertencias de los proveedores y de la industria deben ser monitoreadas regularmente y deben existir procedimientos para garantizar que los parches y / o soluciones se implementen de inmediato.
* El proceso de gestión de vulnerabilidades debe incluir la actualización de la configuración estándar para el firewall con todos los parches o remediaciones identificadas y la configuración actualizada debe aplicarse a todos los firewalls.
* Establecer que los parches críticos deben aplicarse dentro del mes siguiente al lanzamiento por parte del proveedor.

## Mejora continua

* Como las revisiones del firewall deben realizarse al menos cada seis meses, es beneficioso revisar el proceso de revisión del firewall en sí, con el fin de afinar el proceso e identificar mecanismos para reducir el esfuerzo requerido para completar dicha actividad.
* Cuando se evalue el proceso de revisión del firewall se debe identificar qué está funcionando bien y cuáles son las áreas problemáticas.
* Identifique recomendaciones para mejorar las áreas problemáticas.
* Las áreas para mejorar podrían incluir la reducción del esfuerzo requerido para completar las revisiones o abordar el incumplimiento o las brechas en los procesos organizacionales (por ejemplo, gestión de cambios, mantenimiento de configuraciones estándar, gestión de vulnerabilidades y parches).
* Si se determina que la configuración del firewall y las revisiones de reglas requieren un esfuerzo significativo, entonces la organización podría justificar la adquisición de herramientas comerciales para el análisis de reglas de firewall o para revisar configuraciones.
* Una revisión del proceso debe incluir la investigación de problemas recurrentes como diagramas no actualizados, servicios, protocolos o puertos no autorizados en uso que pueden indicar brechas o el incumplimiento de los procesos.
* Para todos los problemas recurrentes identificados, se debe identificar la causa raíz.

1. Tomado de: Methodology for Firewall Reviews for PCI Compliance del SANS Institute [↑](#footnote-ref-1)