GESTIÓN DE LA SEGURIDAD PERIMETRAL

Procedimiento: PR-OTI-007

Versión: 01

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Elaborado por: José Antonio Chacón Calderón Director Oficina de Tecnologías de la Información y la Comunicación **Dueño del proceso**	**Firma:**  Firmado digitalmente por CHACON CALDERON Jose Antonio FAU 20131366028 soft Motivo: Soy el autor del documento Fecha: 28.11.2020 11:52:59 -05:00
Revisado por: Sonia Huamán Lozano Directora Unidad de Modernización y Gestión de la Calidad Laiter Luis García Tueros Director Oficina de Asesoría Jurídica	**Firma:**  Firmado digitalmente por HUAMAN LOZANO Sonia Del Carmen FAU 20131366028 hard Motivo: Soy el autor del documento Fecha: 02.12.2020 08:37:52 -05:00  Firmado digitalmente por GARCIA TUEROS Laiter Luis FAU 20131366028 hard Motivo: Soy el autor del documento Fecha: 02.12.2020 13:21:50 -05:00
Aprobado por: José Percy Barrón López Gerente General Gerencia General	**Firma:**  Firmado digitalmente por BARRON LOPEZ Jose Percy FAU 20131366028 soft Motivo: Soy el autor del documento Fecha: 02.12.2020 22:04:36 -05:00

INDICE

1. OBJETIVO

Gestionar las actividades para garantizar la seguridad perimetral de la red interna de comunicación en el Servicio Nacional de Meteorología e Hidrología del Perú - SENAMHI garantizando la seguridad de la información.

2. ALCANCE

El presente procedimiento es de aplicación y cumplimiento obligatorio para los funcionarios y servidores públicos del SENAMHI.

3. BASE LEGAL

3.1 Ley N° 24031, Ley del Servicio Nacional de Meteorología e Hidrología – SENAMHI, modificado por la Ley N° 27188.
3.2 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, y sus modificatorias.
3.3 Ley N° 29733, Ley de Protección de Datos Personales.
3.4 Ley N° 30096, Ley de Delitos Informáticos.
3.5 Decreto Supremo N° 003-2016-MINAM, que aprueba el Reglamento de Organización y Funciones del SENAMHI.
3.6 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática
3.7 Resolución Jefatural N° 090-95-INEI, que aprueba la Directiva N° 008-95-INEI/SJI “Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública”.
3.8 Resolución Jefatural N° 386-2002-INEI, que aprueba la Directiva N° 016-2002-INEI/DTNP "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública".

4. DEFINCIONES Y SIGLAS

4.1 Amenaza

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicios.

4.2 Análisis de Riesgos

Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

4.3 Base de Datos

Colección de datos organizada de tal modo que sea fácilmente accesible, gestionada y actualizada.

4.4 Controles

Son aquellos mecanismos utilizados para monitorear y controlar acciones consideradas sospechosas y que pueden afectar los activos de información.

4.5 Dirección IP

Conjunto de números, únicos e irrepetibles, que identifica a un equipo informático con la capacidad de conectarse a internet.

4.6 Firewall

Aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

4.7 Firma de antivirus

Archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus.

4.8 Seguridad Perimetral

Es la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

4.9 Seguridad de la información

Consiste en la preservación de su confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de la institución

4.10 Virus

Programa informático escrito para alterar la forma como funciona un equipo informático, sin permiso o conocimiento del usuario.

4.11 Siglas

- UA: Unidad de Abastecimiento
- SistGD: Sistema de gestión documental
- UFN: Unidad Funcional Operativa de Infraestructura Tecnológica
- TIC: Tecnologías de la Información y la Comunicación

5. RESPONSABILIDADES

5.1. Oficina de Tecnologías de la Información y la Comunicación - OTI

5.1.1. Actualizar y formular propuestas de optimización y mejora del presente procedimiento, en el marco de las normas legales correspondientes y las medidas de racionalidad y austeridad en el uso de los recursos públicos.
5.1.2. Gestionar la adquisición de recursos tecnológicos.
5.1.3. Remitir al/la Especialista de la UA el informe de evaluación de soporte como resultado de la validación del servicio realizado por el/la proveedor/a.

6. GENERALIDADES

6.1. Reglas Generales

6.1.1. La OTI gestiona las políticas de seguridad perimetral mencionadas en los ítems a, b, c, d, y e del numeral 6.2.1.1 del presente Procedimiento mediante la herramienta de firewall, con la finalidad de garantizar la seguridad de la información, estabilidad de la red, mitigar el tráfico de red y brindar un óptimo servicio.

6.1.2. En el marco del cumplimiento de las funciones de los usuarios, el acceso a las redes sociales, visualización de videos y descarga de archivos masivos y otras acciones similares, deben contar con la autorización expresa, bajo responsabilidad del/la Director/a del Órgano o Unidad correspondiente, previa evaluación de la OTI.

6.1.3. Los usuarios deben acatar las disposiciones de las políticas de seguridad perimetral que dispongan la OTI, bajo responsabilidad, en caso de incumplimiento.

6.1.4. El usuario debe evitar abrir correos electrónicos de remitentes sospechosos o desconocidos y debe marcarlo como correo no deseado (SPAM), a fin que el equipo de cómputo no sea dañado; en caso de seguir recibiendo estos mensajes se debe informar a la OTI para el análisis respectivo y la solución correspondiente.

6.2. Etapas de la Seguridad Perimetral

La gestión de la seguridad perimetral está compuesto por dos (2) etapas las cuales son: Monitoreo de la seguridad perimetral y configuración de la seguridad perimetral.

6.2.1. Monitoreo de la Seguridad Perimetral:

La OTI monitorea la seguridad perimetral de la red interna del SENAMHI protegiéndola de ataques de redes externas, haciendo uso de las herramientas de firewall, antispam, accesos remotos y antivirus.

6.2.1.1. Firewall

Permite gestionar las políticas de seguridad perimetral de la institución con la finalidad de detectar amenazas que vulneren la red interna de comunicación, garantizar la seguridad de la información, estabilidad de la red y mitigar el tráfico de red.

Las principales políticas de seguridad perimetral gestionadas por la OTI mediante la herramienta firewall son las siguientes:

a) Políticas de acceso a internet:
Acceso a internet con restricción a páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Institución mediante el uso de servidor firewall.

Las excepciones de acceso, serán aprobados por el/la Director/a de la OTI, según sea la necesidad del caso y verificación previa de que las paginas solicitadas no contengan código malicioso.

b) Política ancho de banda:

Cada usuario tiene una capacidad de descarga ancho de banda de 10 Mbps con la finalidad de no congestionar el plan de internet.

Las excepciones de aumento de ancho de banda, será aprobados por el/la Director/a de la OTI, según sea la necesidad del caso y verificación previa de que las paginas solicitadas no contengan código malicioso.

c) Políticas dedicadas:

Capacidad de descarga que supera el ancho de banda permitido, dirigido a usuarios que realizan descargas de datos meteorológicos, hidrológicos, atmosféricos, entre otros.

d) Política de conexión externa:

Consiste en brindar el acceso a los usuarios a los aplicativos cliente servidor desde una ubicación externa al SENAMHI.

e) Política detección contra amenazas (correo institucional):

Consiste en detectar una amenaza mediante el uso del correo electrónico institucional, se detecta de dos (2) maneras; si el usuario ingresa erróneamente cinco (5) veces la contraseña, la cuenta será bloqueada por 30minutos; si el usuario ingresa erróneamente ocho (8) veces la contraseña, será bloqueada la dirección IP y no tendrá acceso a ningún servicio institucional (página web, correo electrónico institucional, SistGD), en estos casos usuario se comunicará con la OTI para la reactivación de la dirección IP.

6.2.1.2. Antispam:

Permite prevenir o restringir la entrega de spam, para ello analiza automáticamente todos los correos electrónicos entrantes enviados al buzón de correo electrónico institucional.

El programa cuenta con una base de datos propia que es actualizada diariamente, solo en el caso que el antispam no detecte un correo malicioso, el/la Especialista de UFN debe analizar el asunto, contenido, y adjunto, para agregar parte del contenido en la base de conocimientos del antispam para un próximo análisis y detección del mismo.

6.2.1.3. Acceso remoto:

El servicio de acceso remoto a la red del SENAMHI permite utilizar los recursos, de la institución, desde localizaciones remotas de forma segura.

La forma de acceder requiere que el usuario remoto tenga conexión a Internet y realice una conexión de VPN (Virtual Private Network). La conexión VPN permite a los usuarios conectarse a la red del SENAMHI utilizando Internet como vínculo de acceso, una vez autenticados, los usuarios tienen un nivel de acceso muy similar al que tienen en la red del SENAMHI.

Se genera accesos remotos para los siguientes casos:

- Acceso desde fuera de la institución, a los recursos informáticos del SENAMHI, bases de datos, servidores y otros que se requiera como parte de sus funciones.
- Acceso por 'Escritorio remoto' a una máquina ubicada en el SENAMHI.

6.2.1.4. Antivirus:

Se cuenta con un antivirus instalado en todos los equipos de los usuarios tanto en la Sede Central como en las Direcciones Zonales del SENAMHI, el cual cumple con los siguientes aspectos:

- Detiene los ataques dirigidos y las amenazas persistentes avanzadas mediante la protección en capas.
- Separa los archivos que están en peligro de los archivos seguros para realizar una detección más rápida y precisa.
- Supervisa en tiempo real el comportamiento de las aplicaciones y detener las amenazas de día cero.
- Mantiene una carga de red reducida con flexibilidad para controlar la cantidad de conexiones de red y el ancho de banda.
- Soporta plataformas físicas y virtuales.
- Limita los posibles efectos de un ataque y proporciona una identificación temprana de los ataques.

6.2.1.5. Soporte de hardware/software de la seguridad perimetral:

Consiste en la verificación de las licencias vigentes de las herramientas descritas en los ítems 6.2.1.1, 6.2.1.2, 6.2.1.3. y 6.2.1.4 del presente procedimiento con la finalidad de gestionar el soporte de los equipos perimetrales con el/la responsable de la UA.

El/la Especialista de la UFN realiza un monitoreo diario de los equipos y determina el estado de los mismos, se requiere de soporte si los equipos presentan los siguientes problemas; por saturación de sus recursos (memoria, CPU, disco duro), o falla de algún componente.

6.3. Configuración de la Seguridad Perimetral

Consiste en la creación de nuevas políticas de seguridad perimetral, y/o eliminación de las ya existentes, esta última debido a que las políticas son temporales. Se le genera backup de firewall cuando existe alguna modificación en las políticas ya establecidas.

7. DESARROLLO

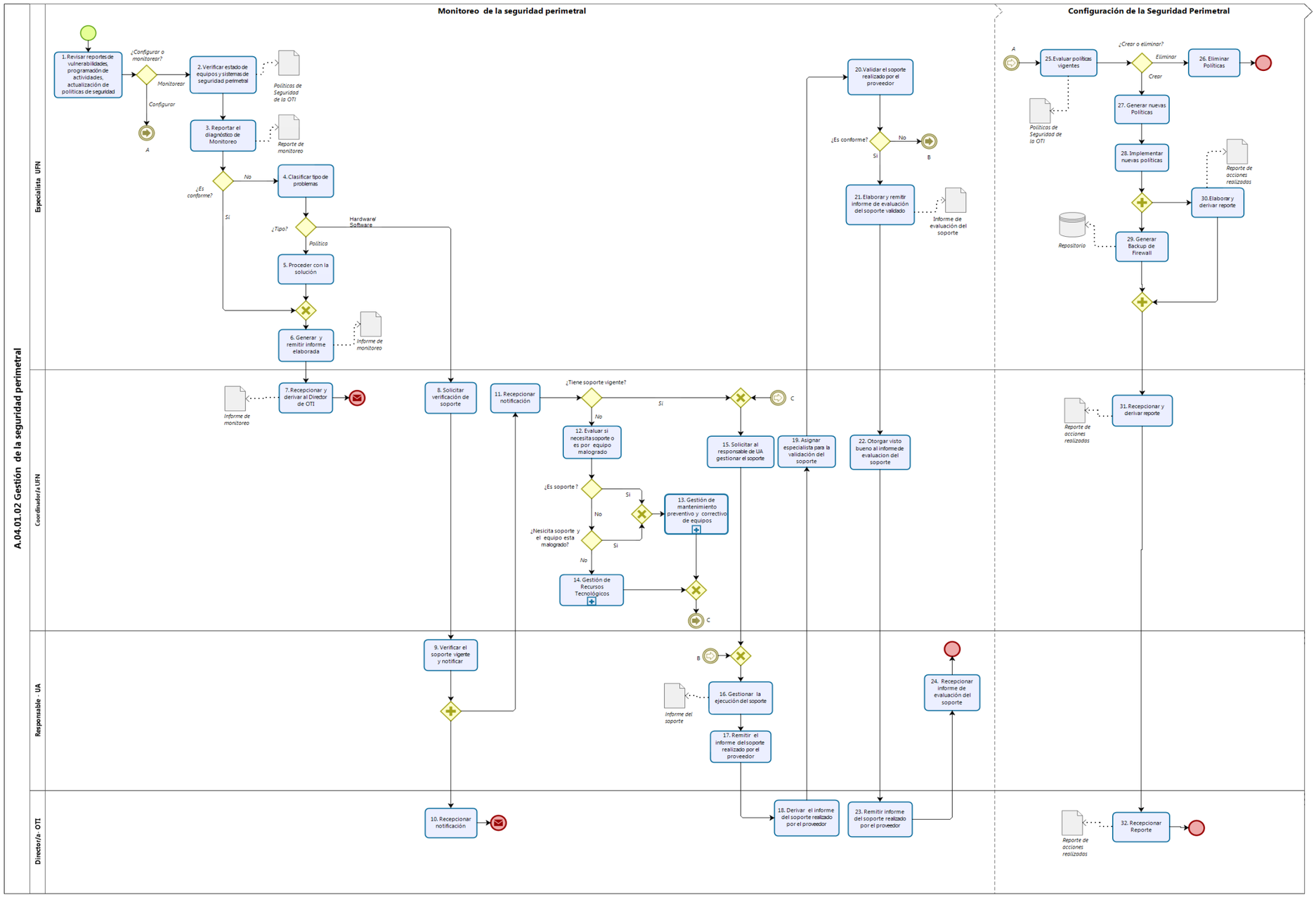
7.1. Requisitos del inicio del procedimiento

Descripción del requisito	Fuente
Reporte de vulnerabilidades detectadas	Software de Alertas a la Seguridad Perimetral y el Antispam
Programación de actividades Información de monitoreo diario de equipos Actualizaciones de políticas de seguridad	Especialista de la UFN

7.2. Proceso relacionado

Todos los procesos identificados en el inventario de proceso vigente que participan en la gestión de seguridad perimetral.

7.3. Diagrama de flujo



7.4. Descripción de actividades

N°	Descripción	Órgano/ Unidad	Responsable	Registros
Monitoreo de la Seguridad Perimetral				
1	Revisar reporte de vulnerabilidades detectadas, programación de actividades y actualizaciones de políticas de seguridad perimetral. **¿Configurar o monitorear?** **Configurar: continuar con la Actividad N° 25** **Monitorear: continuar con la Actividad N° 2** Nota: el reporte de alerta de vulnerabilidades es generado por Software de Alertas a la Seguridad Perimetral y el Antispam.	OTI	Especialista de la UFN	– – –
2	Verificar el estado de equipos informáticos y sistemas de seguridad perimetral.	OTI	Especialista de la UFN	Políticas de Seguridad de la OTI
3	Reportar el diagnóstico de monitoreo de los equipos informáticos y sistemas de seguridad perimetral. **¿Es conforme?** **Si: continuar con la Actividad N° 7** **No: continuar con la Actividad N° 4**	OTI	Especialista de la UFN	Reporte de Monitoreo
4	Clasificar por tipo de problema (política, hardware, software). **¿Qué tipo de problema es?** **Política: Continuar con la Actividad N° 5** **Hardware/Software: Continuar con la Actividad N° 8**	OTI	Especialista de la UFN	– – –
5	Proceder con la solución al problema de vulneración a las políticas de seguridad detectado.	OTI	Especialista de la UFN	– – –
6	Generar y remitir informe de monitoreo con las acciones realizadas al/la Coordinador/a de la UFN.	OTI	Especialista de la UFN	Informe de monitoreo
7	Recepcionar y derivar el informe del monitoreo al/la Director/a de la OTI.	OTI	Coordinador/a de la UFN	Informe de monitoreo

N°	Descripción	Órgano/ Unidad	Responsable	Registros
8	Solicitar verificación de garantía del hardware/software al/la Especialista de la UA.	OTI	Coordinador/a de la UFN	– – –
9	Verificar garantía y notificar al/la Coordinador/a de la UFN y al/la Director/a de la OTI.	UA	Responsable de la UA	– – –
10	Recepcionar notificación de garantía del hardware/software.	OTI	Director/a de la OTI	– – –
11	Recepcionar notificación de garantía del hardware/software. **¿Garantía vigente?** **Si: continuar con la Actividad N° 15** **No: continuar con la Actividad N° 12**	OTI	Coordinador/a de la UFN	– – –
12	Evaluar si necesita soporte o es por equipo malogrado. **¿Es soporte?** **Si: continuar con la Actividad N° 13** **No: continuar con la siguiente pregunta** ¿Necesita soporte y el equipo esta malogrado? **Si: continuar con la Actividad N°13** **No: continuar con la Actividad N°14**	OTI	Coordinador/a de la UFN	– – –
13	Iniciar con el **Proceso de A.04.02.02 Gestión de mantenimiento preventivo y correctivo de equipos informáticos y redes de comunicaciones de datos**, según lo establecido en el procedimiento PR-OTI-003. Una vez adquirido el servicio, continuar con la Actividad N° 15.	OTI	Coordinador/a de la UFN	– – –
14	Iniciar con el **Proceso de A.04.02.07 Gestión de recursos tecnológicos** para la adquisición de recursos TIC. Una vez adquiridos los recursos tecnológicos, continuar con la Actividad N° 15.	OTI	Director/a de la OTI	– – –
15	Solicitar al/la responsable de la UA gestionar el soporte.	OTI	Coordinador/a de la UFN	– – –

N°	Descripción	Órgano/ Unidad	Responsable	Registros
16	Gestionar la ejecución del soporte.	UA	Responsable de la UA	Informe del mantenimiento
17	Remitir el informe del soporte realizado por el proveedor.	UA	Responsable de la UA	– – –
18	Derivar el informe del soporte realizado por el proveedor al/la Coordinador/a de la UFN.	OTI	Director/a de la OTI	– – –
19	Asignar especialista para la validación del soporte.	OTI	Coordinador/a de la UFN	– – –
20	Validar el soporte realizado por el proveedor. **¿Es conforme?** **Si: continuar con la actividad N° 21** **No: Reiniciar con la actividad N° 16**	OTI	Especialista de la UFN	– – –
21	Elaborar y remitir informe de evaluación del soporte realizado por el proveedor.	OTI	Especialista de la UFN	Informe de evaluación del soporte
22	Otorgar visto bueno al informe de evaluación del soporte.	OTI	Coordinador/a de la UFN	– – –
23	Remitir informe del soporte elaborado por el proveedor al/la Responsable de la UA.	OTI	Director/a de la OTI	– – –
24	Recepcionar el informe de evaluación del soporte.	UA	Responsable de la UA	– – –
Configuración de Seguridad Perimetral				
25	Evaluar políticas de seguridad perimetral vigentes. **¿Crear o eliminar las políticas vigentes?** **Eliminar: continuar con la actividad N° 26** **Crear: continuar con la actividad N° 27**	OTI	Especialista de la UFN	Políticas de Seguridad de la OTI
26	Eliminar políticas de Seguridad Perimetral.	OTI	Especialista de la UFN	– – –
27	Generar nuevas políticas de Seguridad Perimetral.	OTI	Especialista de la UFN	– – –

N°	Descripción	Órgano/ Unidad	Responsable	Registros
28	Implementar nuevas políticas de Seguridad Perimetral.	OTI	Especialista de la UFN	– – –
29	Generar Backup de Firewall según lo establecido en el procedimiento de PR-OTI-002 Gestión de Backup.	OTI	Especialista de la UFN	Backup de Firewall (configuración de Seguridad Perimetral)
30	Elaborar y derivar reporte de las acciones realizadas al/la Coordinador/a de la OTI.	OTI	Especialista de la UFN	– – –
31	Recepcionar y derivar reporte de las acciones realizadas al/la Director/a de la OTI.	OTI	Coordinador/a de la UFN	Reporte de acciones realizadas
32	Recepcionar reporte de las acciones realizadas **Finalizar.**	OTI	Director/a de la OTI	Reporte de acciones realizadas

8. REGISTROS

Denominación	Código
Reporte de Monitoreo	S/C
Informe de monitoreo	S/C
Informe de evaluación del soporte	S/C
Reporte de acciones realizadas	S/C

9. TABLA HISTÓRICA DE CAMBIOS

Versión	Fecha	Detalle de cambios
01	--	Versión inicial