PROCEDIMIENTO	Código: P-TI-08
	Versión: 01
	Vigencia:

ProInversión
Agencia de Promoción de la Inversión Privada - Perú

GESTIÓN DE INCIDENCIAS DE SEGURIDAD PERIMETRAL

	Nombres y Apellidos	Cargo	Firma	Fecha
Elaborado por:	Manuel Aguilar Cori	Analista en Seguridad de la Información del Área de Tecnologías de la Información		
	Gonzalo Fernández Irigoin	Analista de redes y comunicaciones del Área de Tecnologías de la Información		
Revisado por:	Víctor Chávez Gómez	Jefe de Tecnologías de la Información		
	Martín Bermúdez Peláez	Especialista en Planeamiento y Racionalización de la Oficina de Planeamiento y Presupuesto	BERMUDEZ PELAEZ Luis Martin FAU 20380799643 soft Firmado digitalmente por BERMUDEZ PELAEZ Luis Martin FAU 20380799643 soft Fecha: 2020.12.04 15:24:34 -05'00'	
Aprobado por:	Carlos Albán Ramírez	Jefe de la Oficina de Administración		

ÍNDICE

1. Objetivo

Establecer las actividades para la Gestión de incidencias de seguridad perimetral de PROINVERSIÓN.

2. Alcance

Este procedimiento comprende desde solicitud de creación o modificación de políticas de seguridad en el equipo de seguridad perimetral, hasta la comunicación de la finalización de la solicitud.

Involucra a todo el personal del Área de Tecnologías de la Información.

3. Siglas y Definiciones

Para efectos del presente procedimiento:

3.1. Siglas

- OA: Oficina de Administración
- TI: Tecnologías de Información

3.2. Definiciones

Para efectos del presente procedimiento, se establecen las siguientes definiciones:

- **Equipos de seguridad perimetral:** Equipos instalados en la frontera de la red local (firewall y reporteador) protege la red local de la externa, a través de políticas de seguridad predefinidas.

- **Incidencias de seguridad perimetral:** Evento que pone el peligro el tráfico seguro de la red local a Internet o viceversa.

- **Red local:** Conjunto de equipos de cómputo interconectados, que pertenecen a la misma organización en un área relativamente pequeña.

- **Sistema de Seguridad:** Aplicativo informático instalado en el equipo de seguridad perimetral (firewall), permite la configuración del tráfico de datos tanto de entrada y salida de la red local.

4. Base Legal y Referencia Documental

- 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, la cual debe ser implementada y adecuada en un plazo máximo de dos años por parte de las entidades integrantes del Sistema Nacional de Informática. Aprobada con la Resolución Ministerial N° 004-2016-PCM.

- Norma Técnica Peruana NTP-ISO/IEC 27002:2017 Lineamientos para la seguridad de la información en las organizaciones y prácticas de gestión para la seguridad de la información, incluyendo la selección, la implementación y la gestión de controles tomando en consideración los riesgos del entorno para la seguridad de la información de la organización.

- Directiva N° 002-2010-PROINVERSION- "Administración de la seguridad de los bienes y servicios informáticos". Aprobada con Resolución de Dirección Ejecutiva N° 060-2010.

- Norma Técnica Nº 001-2018-PCM/SGP, "Implementación de la Gestión por Procesos en las Entidades de la Administración Pública" aprobada mediante la Resolución de Secretaria de Gestión Pública N° 006-2018-PCM-SGP.

- "Metodología para la Implementación de la Gestión por Procesos en PROINVERSION", aprobada con la Resolución de Secretaría General N° 81-2019, el 15 de mayo de 2019.

5. Responsabilidades

5.1. Del Analista en seguridad de la información

a. Revisar tráfico de información en la red en la red local interna.
b. Evaluar y dar solución a las incidencias de seguridad perimetral.
c. Contactar al proveedor de servicios de equipos de seguridad perimetral y servicios de soporte del firewall.
d. Dar seguimiento proveedor de servicios de equipo de seguridad perimetral y servicios de soporte del firewall.
e. Verificar y registrar solución a incidencias de seguridad perimetral.
f. Archivar bitácoras y reportes.
g. Analizar la solicitud de acceso a páginas o servicios en internet.
h. Verificar la atención a la solicitud de accesos a páginas o servicios en internet.
i. Crear o modificar la política de seguridad en el firewall.

5.2. Del Jefe de Tecnologías de la Información

a. Revisar bitácora de equipo de seguridad perimetral.
b. Solicita la creación o modificación de la política de seguridad en el firewall que permita atender el acceso solicitado.

5.3. Del Director o Jefe (área usuaria)

a. Solicitar acceso a páginas o servicios en internet.
b. Realizar pruebas de funcionamiento de la política en el firewall.

6. Generalidades

6.1. De las incidencias de seguridad perimetral

Algunas incidencias en el Firewall son:

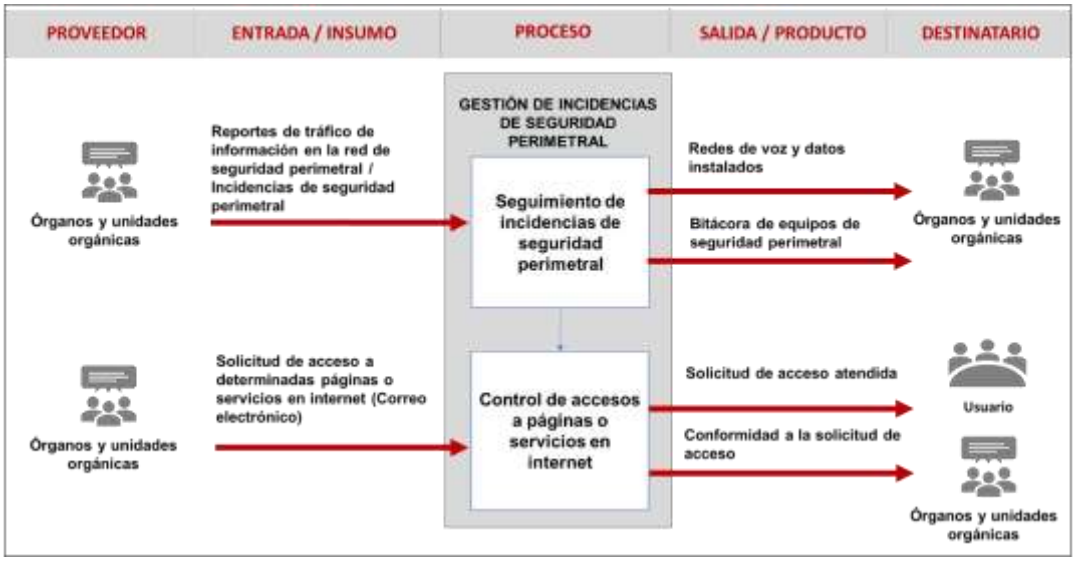
- Falta de actualizaciones de software (firmware).
- Los recursos del procesador y memoria por encima del 70%.

6.2. De los niveles de procesos

- Proceso de Nivel 0: Gestión de Tecnologías de la Información
- Proceso de Nivel 1: Gestión de accesos a servicios de tecnologías de la información
- Proceso de Nivel 2: Gestión de Incidencias de Seguridad Perimetral

6.3. Esquema del proceso

Las entradas y salidas del proceso de Gestión de Incidencias de Seguridad Perimetral, así como sus proveedores y destinatarios del proceso final, se visualiza en el siguiente esquema.



7. Procedimiento

7.1. Seguimiento de incidencias de seguridad perimetral

N°	Actividad	Órgano o Unidad Orgánica	Rol	Descripción de la actividad
1	**Revisar tráfico de información en la red en la red local interna**	OA (Área de TI)	Analista en seguridad de la información	Diariamente revisa los reportes de tráfico de información en la red local interna, recibidos por **correo electrónico**. Identifica el tráfico inusual de información o incidencias de seguridad perimetral.
2	**Evaluar y dar solución a las incidencias de seguridad perimetral**	OA (Área de TI)	Analista en seguridad de la información	Evaluar la solución a la incidencia de seguridad perimetral identificada.

N°	Actividad	Órgano o Unidad Orgánica	Rol	Descripción de la actividad
				¿Es factible solucionarlo internamente? **SI:** Da solución a las incidencias de seguridad perimetral. Ir a la actividad 5. **NO:** Ir a la actividad 3.
3	**Contactar al proveedor de servicios de equipos de seguridad perimetral**	OA (Área de TI)	Analista en seguridad de la información	Contacta al proveedor de servicios de equipo de seguridad perimetral, indicando la incidencia **de seguridad perimetral** detectada a través de un **correo electrónico** con copia al Jefe de TI para conocimiento. Recibe del proveedor un número de ticket de atención de la incidencia.
4	**Dar seguimiento proveedor de servicios de equipo de seguridad perimetral**	OA (Área de TI)	Analista en seguridad de la información	Dar seguimiento al estado de la incidencia de seguridad perimetral hasta la solución de la misma, a través del número de ticket de atención y coordinaciones con el proveedor de servicios de equipos de seguridad perimetral.
5	**Verificar y registrar solución a incidencias de seguridad perimetral**	OA (Área de TI)	Analista en seguridad de la información	Verifica solución a incidencias de seguridad perimetral. **¿Es conforme?** **SI:** Registra las acciones realizadas para la solución en la **Bitácora de equipos de seguridad perimetral** y remite copia a jefe de TI. Ir a la actividad 6. **NO:** Comunica al proveedor de soporte de servicios de equipos de seguridad perimetral. Ir a la actividad 3.
6	**Revisar bitácora de equipo de seguridad perimetral**	OA (Área de TI)	Jefe de Tecnologías de la Información	Revisa la información consignada en la **Bitácora de equipo de seguridad perimetral** **¿Está conforme?** **SI:** Firma y remite a Analista en seguridad de la Información.

N°	Actividad	Órgano o Unidad Orgánica	Rol	Descripción de la actividad
				NO: Devuelve a Analista en seguridad de la Información, para su modificación. Ir la actividad 5
7	**Archivar bitácoras y reportes**	OA (Área de TI)	Analista en seguridad de la información	Archiva las **bitácoras de equipos de seguridad perimetral** y los reportes que indican la incidencia se ha resuelto. *Fin de proceso.*

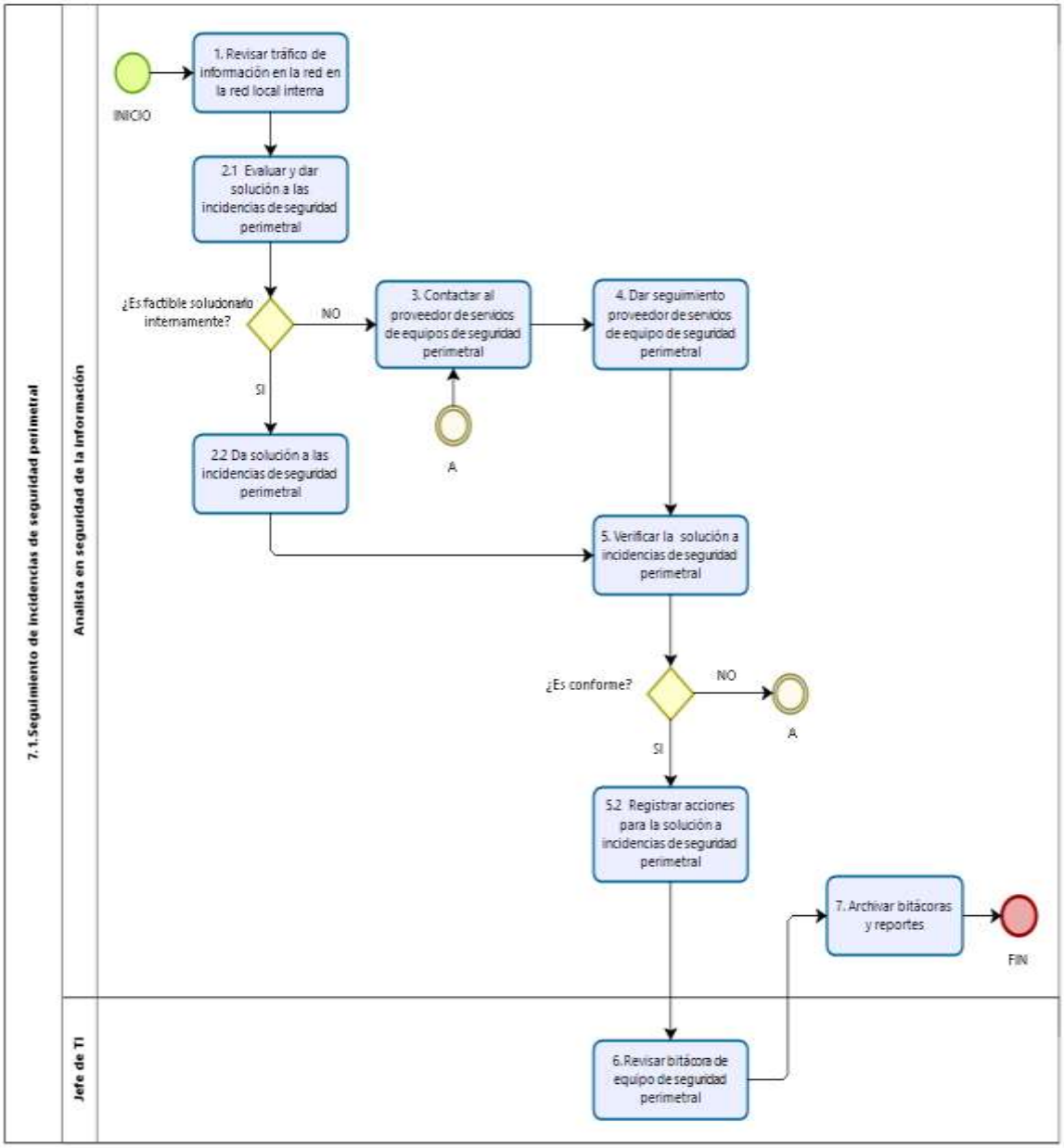
7.2. Control de accesos a páginas o servicios en internet

N°	Actividad	Órgano o Unidad Orgánica	Rol	Descripción de la actividad
1	**Solicitar acceso a páginas o servicios en internet**	Órgano o Unidad Orgánica (áreas usuarias)	Director o jefe	Solicitar el acceso a determinadas páginas o servicios en internet, sustentando la solicitud, mediante **correo electrónico.**
2	**Analizar la solicitud**	OA (Área de TI)	Jefe de TI	Solicita al Analista en Seguridad de la Información crear o modificar la política de seguridad en el firewall que permita atender el acceso solicitado.
		OA (Área de TI)	Analista en seguridad de la información	Recibe y analiza solicitud para crear o modificar la política de seguridad en el firewall que permita atender el acceso solicitado. **¿Es factible crear o modificar la política de seguridad internamente?** **SI**: Ir a la actividad 6. NO: Ir a la Actividad 3
3	**Contactar al proveedor de servicios de soporte del firewall**	OA (Área de TI)	Analista en seguridad de la información	Contacta al proveedor de servicios de equipo de seguridad perimetral, servicios de soporte del firewall, para la creación o modificación de la política de seguridad en el firewall, que permita atender el acceso solicitado. Recibe del proveedor un número de ticket de atención de la solicitud.

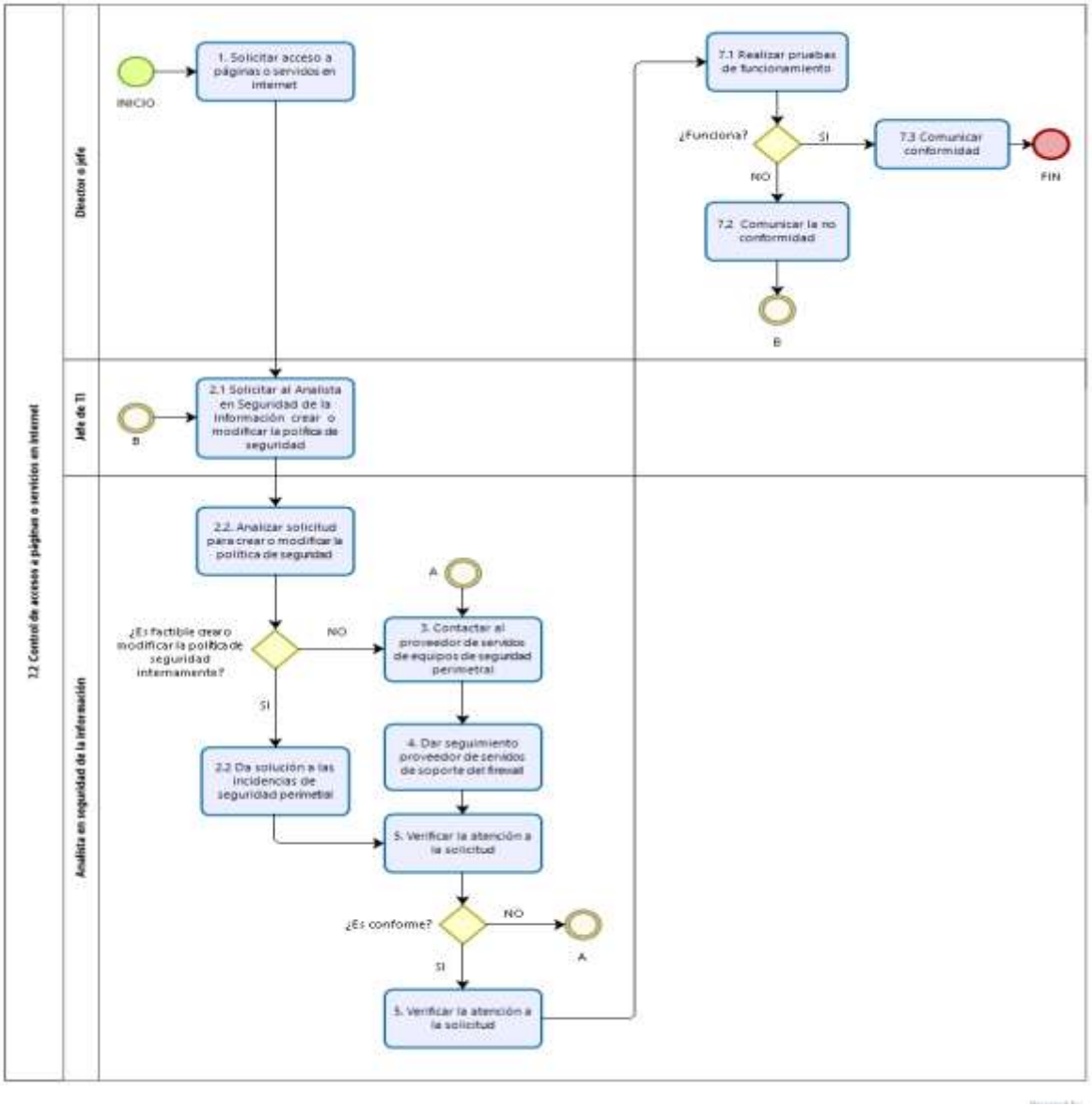
N°	Actividad	Órgano o Unidad Orgánica	Rol	Descripción de la actividad
4	**Dar seguimiento proveedor de servicios de soporte del firewall**	OA (Área de TI)	Analista en seguridad de la información	Dar seguimiento, a través del número de ticket de atención y coordinaciones con el proveedor de servicios de soporte del firewall, hasta recibir el correo electrónico con la solicitud atendida.
5	Verificar la atención a la solicitud	OA (Área de TI)	Analista en seguridad de la información	Verifica la atención de la solicitud y comunica al Jefe de TI **¿Es conforme?** **SI:** Solicita que realice la prueba de funcionamiento. Ir a la Actividad 7. **NO:** Comunica al proveedor de soporte del firewall la no conformidad de funcionamiento de la política de seguridad. Para su revisión con el mismo número de ticket de atención. Ir a la Actividad 3.
6	Crear o modificar la política de seguridad en el firewall	OA (Área de TI)	Analista en seguridad de la información	Crea o modifica la política de seguridad en el firewall. Comunica al área usuaria que solicitó el pedido, para que realice las pruebas de funcionamiento.
7	Realizar pruebas de funcionamiento y comunicar	Órgano o Unidad Orgánica (áreas usuarias)	Director o jefe	Realiza pruebas de funcionamiento de la política en el firewall a través del acceso solicitado. **¿Funciona?** **NO:** Comunica al Analista en Seguridad de la Información, la no conformidad. Ir a la actividad 2. **SI:** Comunica al Analista en seguridad de la información la conformidad. *Fin de proceso*.

8. Flujograma

8.1. Seguimiento de incidencias de seguridad perimetral



8.2. Control de accesos a páginas o servicios en internet



9. Registros

- Correo electrónico de reportes de tráfico de información en la red local interna.
- Bitácora de equipos de seguridad perimetral.
- Correo electrónico que solicita el acceso a determinadas páginas o servicios en internet, sustentando la solicitud.
- Comunicación al área usuaria, para que realice las pruebas de funcionamiento del acceso solicitado.
- Comunicación la conformidad o no conformidad de la solicitud de acceso.

10. Control de cambios

Versión	Fecha	Descripción del cambio
01		Versión Inicial