INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

OFICINA TÉCNICA DE INFORMÁTICA

PROCEDIMIENTO PARA INSTALACIÓN, ACTUALIZACIÓN Y MONITOREO DE ANTIVIRUS EN EL INEI - OTIN

Código: PRA-001-OTIN-2017-V01

PROCEDIMIENTO ADMINISTRATIVO		
NOMBRE DEL PROCEDIMIENTO: PROCEDIMIENTO PARA INSTALACIÓN, ACTUALIZACIÓN Y MONITOREO DE ANTIVIRUS EN EL INEI - OTIN		
CODIGO: PRA-001-OTIN-2017-V01		**VERSION:** 01
PROCESO AL QUE PERTENECE: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
Elaborado por: Unidad de Infraestructura TI y Unidad de Calidad, Procesos y Seguridad de la Información		**Aprobado por:** Director Técnico de la Oficina Técnica de Informática
Nombre:		**Nombre:** Manuel Matos Alvarado
Marco Calderón Lozano	Jessica Raquel Perez Tapia	
Fecha:		**Fecha:**
Firma		**Firma**

TABLA DE CONTENIDO

"PROCEDIMIENTO PARA INSTALACIÓN, ACTUALIZACIÓN Y MONITOREO DE ANTIVIRUS EN EL INEI - OTIN"

1. OBJETIVO

Proteger las estaciones de trabajo, servidores y los dispositivos móviles corporativos frente a las nuevas amenazas. El Antivirus proporciona una Infraestructura de seguridad que protege los equipos físicos y virtuales, integrada en una estación de trabajo única, implementados y gestionados conjuntamente desde una consola, dependiendo de la ubicación física.

2. ALCANCE

El presente documento considera los procedimientos para la instalación, actualización y monitoreo del agente Antivirus en las estaciones de trabajo, equipos informáticos y servidores.

Está dirigido al personal de la OTIN, cuya administración y monitoreo está a cargo de la Unidad de Infraestructura a través del administrador de la consola de antivirus.

Se evaluará:

- Acceso a la consola de antivirus
- Verificación de registros de Actualización de PC, equipo portátil y Servidor a través de una consola.
- Registros de actualización de componentes del agente
- Instalación del agente de Antivirus
- Actualización automático y manual de los agentes de antivirus
- Generación de reportes del estado de PC, equipo portátil y servidores ante un ataque de virus.

3. RESPONSABLES

3.1. Administrador de Red

- Verificar que la última actualización de la firma de antivirus se haya descargado correctamente en el servidor.
- Responsable de instalar los agentes de antivirus en los servidores físicos y virtuales.
- Verificar que la actualización de los componentes se haya aplicado a todos los agentes registrados en la consola de antivirus.

- Monitorear que todos los equipos informáticos de escritorio (PCs, laptops) y servidores de la red INEI y externos (Oficinas Departamentales y Sede Lima) tenga actualizada la BD de antivirus con el agente vigente.
- Generar relación de servidores que no hayan podido conectarse con el servidor de antivirus.
- Proporcionar a soporte la relación de equipos informáticos que no hayan podido conectarse con el servidor de antivirus.

3.2. Soporte Técnico

- Encargado de instalar los agentes de antivirus en las nuevas PCs y/o el traslado entre sedes.
- Responsable de identificar las ubicaciones físicas de las estaciones de trabajo de los usuarios y realizar la actualización manualmente a través del agente de antivirus.
- Se encargan de realizar las reinstalaciones del antivirus de aquellas PCs que no puedan realizar actualizaciones.
-

4. DEFINICIONES

Entiéndase para efectos del presente procedimiento, lo siguiente:

a) **Consola de Antivirus:** Sitio web del antivirus donde se administra los agentes, tanto en estaciones de trabajo, servidores físicos y virtuales.

b) **Firma de Antivirus:** Componente de actualización que debe de descargarse en el servidor y ejecutarse en todos los agentes registrados en la consola de antivirus.

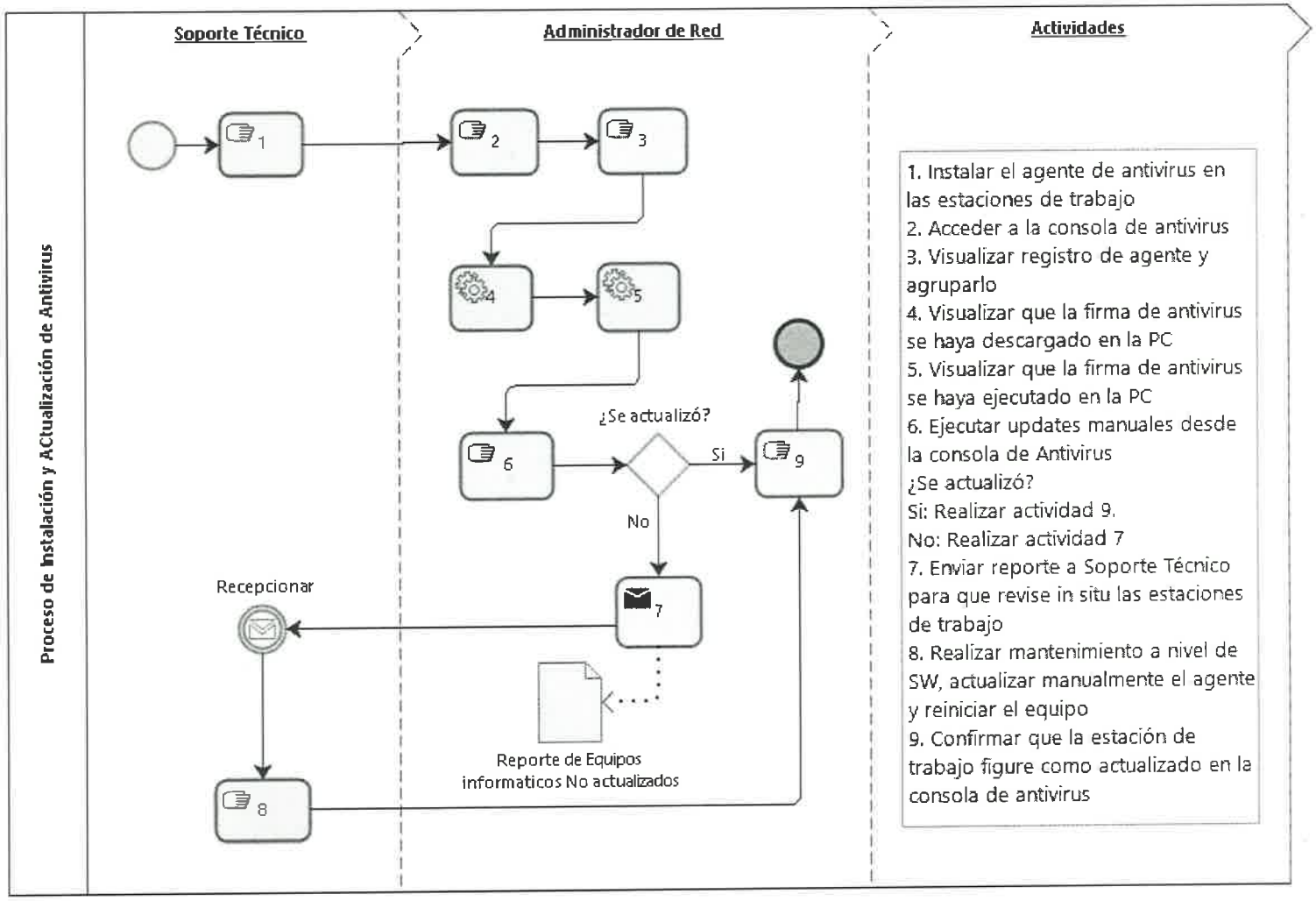
c) **Agente de Antivirus:** Agente de puesto de trabajo único, que se instala en los puestos de trabajo y que recibe actualizaciones diarias para mantener protegido el sistema y los datos de un equipo, protege de vulnerabilidades como Virus, Malware, Spyware, Grayware, Web reputation.

d) **Update:** Actualización de la firma del agente de antivirus.

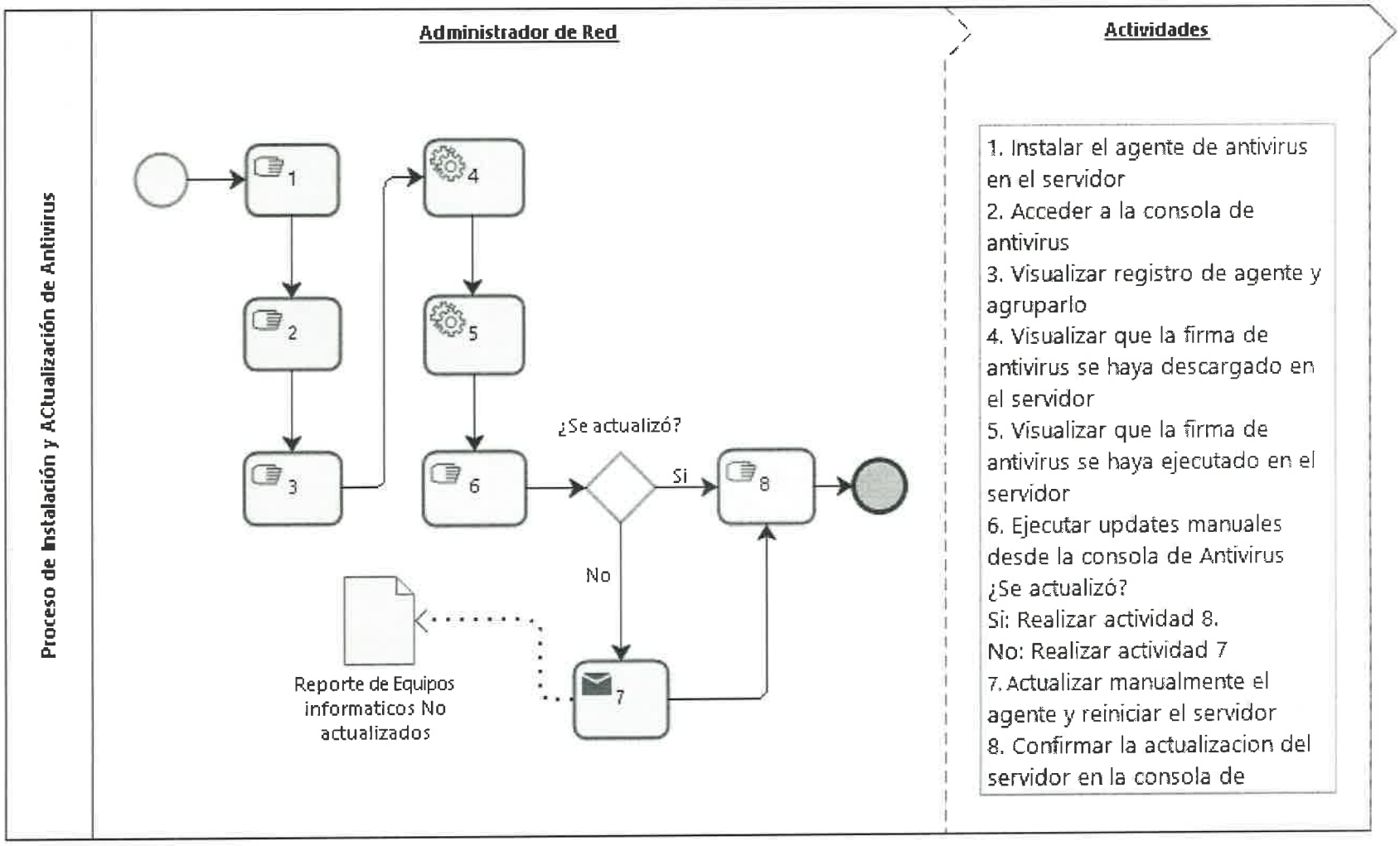
5. DESARROLLO

5.1. FLUJO

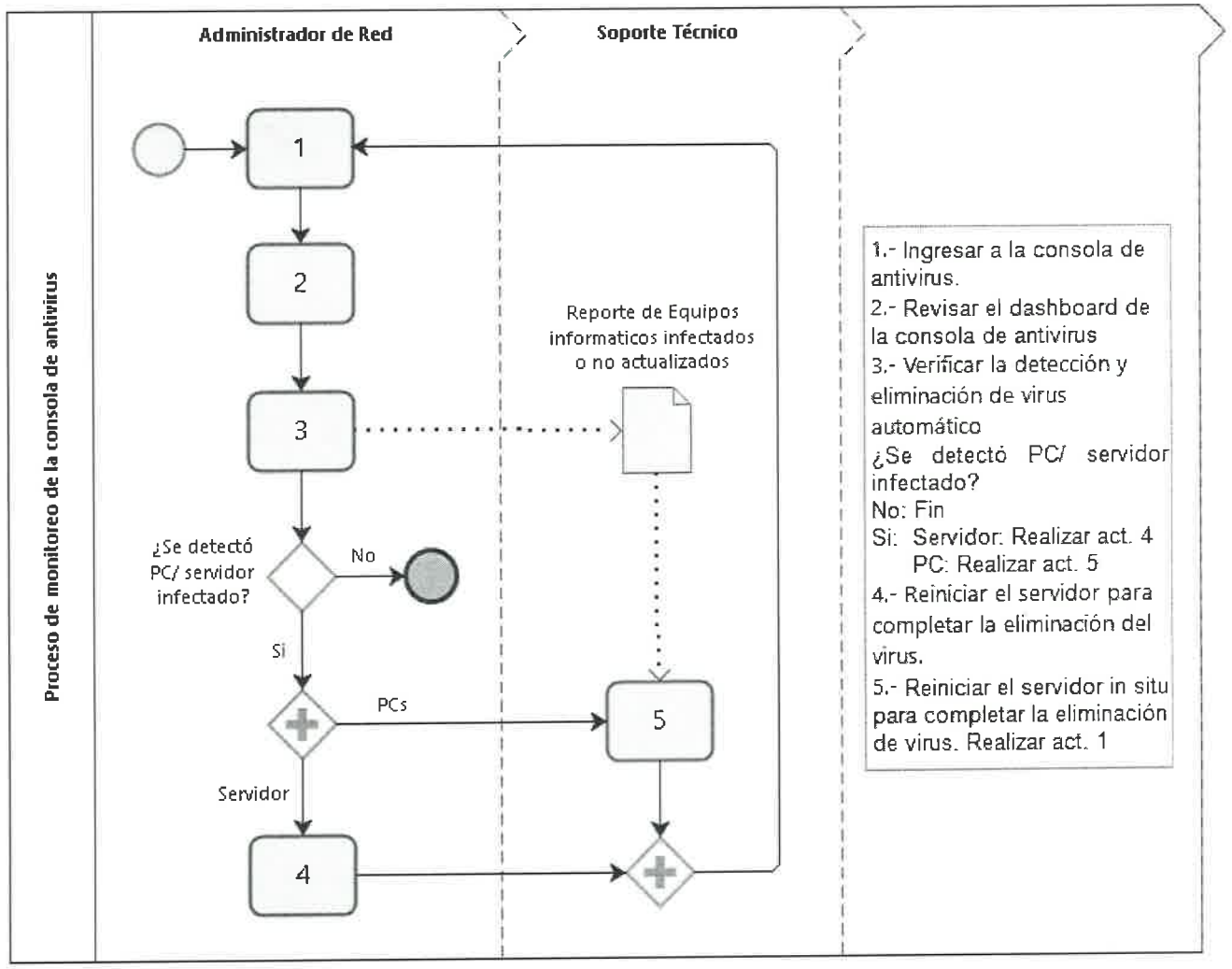
5.1.1. Equipos informáticos de escritorio que conforman el Centro de Datos del INEI



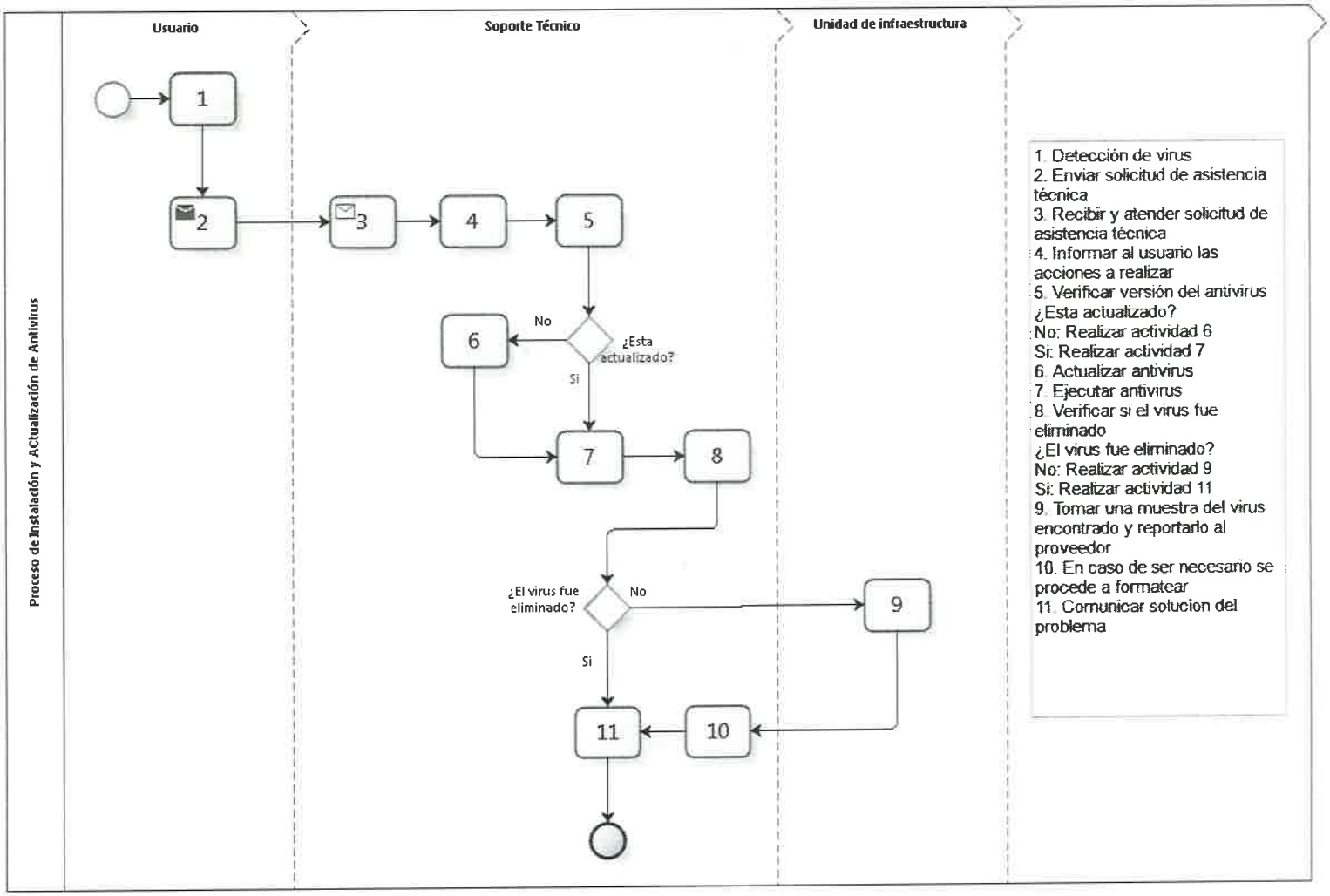
5.1.2. Servidores que conforman el Centro de Datos del INEI



5.1.3. Monitoreo de la consola de antivirus que conforma el Centro de Datos INEI



5.1.4. Detección de virus por parte del Usuario



5.2. DESCRIPCIÓN DE LAS ACTIVIDADES

5.2.1. Equipos informáticos de escritorio que conforman el Centro de Datos del INEI

N°	Responsable	Actividades
1	Soporte Técnico	Instalar el agente de antivirus en las estaciones de trabajo
2	Administrador de Red	Acceder a la Consola de Antivirus
3	Administrador de Red	Visualizar que el agente se haya registrado correctamente en la consola de antivirus y agruparlo en su grupo correspondiente
4	Administrador de Red	Visualizar que firma de antivirus se haya descargado en la consola del servidor, revisar que este actualizado a la fecha
5	Administrador de Red	Visualizar que la firma de antivirus se haya ejecutado en los Agentes Registrados
6	Administrador de Red	Ejecutar actualizaciones (updates) manuales desde la consola de Antivirus
		¿Se actualizó? Si: Realizar actividad 9. No: Realizar actividad 7.
7	Administrador de Red	Enviar reporte (Anexo 01) al área de Soporte Técnico para que revise in situ las estaciones de trabajo,
8	Soporte Técnico	Realizar mantenimiento a nivel de software, actualizar manualmente el agente y reiniciar el equipo
9	Administrador de Red	Confirmar que la estación de trabajo figure como actualizado en la consola de antivirus

5.2.2. Servidores que conforman el Centro de Datos del INEI

N°	Responsable	Actividades
1	Administrador de Red	Instalar el agente de antivirus en el servidor
2	Administrador de Red	Acceder a la Consola de Antivirus
3	Administrador de Red	Visualizar que el agente se haya registrado correctamente en la consola de antivirus y agruparlo en su grupo correspondiente
4	Administrador de Red	Visualizar que firma de antivirus se haya descargado en el servidor, revisar que este actualizado a la fecha
5	Administrador de Red	Visualizar que la firma de antivirus se haya ejecutado en el servidor.
6	Administrador de Red	Ejecutar actualizaciones (updates) manuales desde la consola de Antivirus
		¿Se actualizó? Si: Realizar actividad 8. No: Realizar actividad 7
7	Administrador de Red	Actualizar manualmente el agente y reiniciar el servidor que figura en el reporte (anexo 01)
8	Administrador de Red	Confirmar la actualización del servidor en la consola de antivirus

5.2.3. Monitoreo de la consola de antivirus que conforma el Centro de Datos INEI

N°	Responsable	Actividades
1	Administrador de Red	Ingresar a la consola de antivirus.
2	Administrador de Red	Revisar el tablero (dashboard) de la consola de antivirus

N°	Responsable	Actividades
3	Administrador de Red	Verificar la detección y eliminación de virus automático, con posible detección de equipos y servidores infectados generado en el reporte (Anexo 01)
		¿Se detectó PC/ servidor infectado? No: Fin Si: Servidor: Realizar actividad 4 PC: Realizar actividad 5
4	Administrador de Red	Reiniciar de ser necesario el servidor para completar la eliminación de virus.
5	Soporte Técnico	Reiniciar de ser necesaria la PC in situ para completar la eliminación de virus. Realizar actividad 1

5.2.4. Detección de virus en la PC del Usuario

N°	Responsable	Actividades
1	Usuario	El usuario visualiza el mensaje de alerta emitido por el antivirus ante una posible amenaza.
2	Usuario	Enviar solicitud de asistencia técnica mediante el sistema de servicios informáticos
3	Soporte Técnico	Recibir y atender solicitud de asistencia técnica que solicitó el usuario
4	Soporte Técnico	Informar al usuario las acciones a realizar sobre su solicitud de asistencia técnica.
5	Soporte Técnico	Verificar la versión del agente antivirus del equipo informático.
		¿Está actualizado? No: Realizar actividad 6 Si: Realizar actividad 7
6	Soporte Técnico	Actualizar antivirus en el equipo informático que requiere asistencia técnica

N°	Responsable	Actividades
7	Soporte Técnico	Ejecutar antivirus en el equipo informático
8	Soporte Técnico	Verificar si el virus fue eliminado del equipo informático dañado.
		¿El virus fue eliminado? Si: Realizar actividad 11 No: Realizar actividad 9
9	Unidad de infraestructura	Tomar una muestra del virus encontrado y reportarlo al proveedor
10	Soporte Técnico	En caso de ser necesario se procede a formatear para la restauración del equipo informático
11	Soporte Técnico	Comunicar solución del problema

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática ELMER PEREZ ESPINOZA

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA V° B° OFICINA TECNICA DE INFORMATICA EDUARDO CORILLA BACILIO

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA Oficina Técnica de Informática FERNANDO ENCARNACION MENDOZA

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA V° B° Michael Málaga Matasich -INEI-

INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA FRANK DAVID MENDOZA

6. REGISTROS

- ANEXO 01: Reporte de Equipos informáticos no actualizados.

7. ANEXOS

ANEXO 01: Reporte de Equipos informáticos no actualizados.

Domain	Endpoint	IP Address	Connection Status	Platform	Smart Scan Agent Pattern	Last Startup	Last Shutdown	Agent Installation	Fecha de Revisión

Para el Reporte de Equipos informáticos no actualizados se requiere los siguientes campos

- ✓ Dominio: Domain
- ✓ Usuario: Endpoint
- ✓ Dirección IP: IP Address
- ✓ Estado: Connection Status
- ✓ Sistema Operativo: Platform
- ✓ Patrón de actualización: Smart Scan Agent Pattern
- ✓ Ultimo encendido: Last Startup
- ✓ Ultimo apagado: Last Shutdown
- ✓ Fecha de instalación de agente: Agent Installation
- ✓ Fecha de revisión: Este campo lo llena Soporte Técnico.