Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0305 Versión: ***03*** Fecha: 22/12/2022

NOMBRE DEL PROCEDIMIENTO	Monitoreo y control de seguridad informática

APROBACIÓN		
Nombre y cargo	**Órgano o Unidad Orgánica**	**Firma y sello**
Elaborado por: Zico Alexis Yacila Espinoza Jefe de la Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: YACILA ESPINOZA Zico Alexis FAU 20521286769 soft Cargo: Jefe de la Oficina de Tecnologías de la Información Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Revisado por: Elvis Romel Palomino Pérez Jefe de la Oficina de Planeamiento y Presupuesto	Oficina de Planeamiento y Presupuesto	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: PALOMINO PEREZ Elvis Romel FAU 20521286769 soft Cargo: Jefe de la Oficina de Planeamiento y Presupuesto Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Revisado por: Gonzalo Pinto Bazurco Mendoza Jefe de la Oficina de Asesoría Jurídica	Oficina de Asesoría Jurídica	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: PINTO BAZURCO MENDOZA Gonzalo FAU 20521286769 soft Cargo: Jefe de la Oficina de Asesoría Jurídica Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Aprobado por: Miriam Alegría Zevallos Gerenta General	Gerencia General	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: ALEGRIA ZEVALLOS Miriam FAU 20521286769 soft Cargo: Gerenta General Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento

Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0305 Versión: ***03*** Fecha: 22/12/2022

CONTROL DE CAMBIOS		
Versión	**Sección del Procedimiento**	**Descripción del cambio**
00	-	Versión inicial del procedimiento[1]
01	Todas las secciones	- Se actualiza el alcance. - Se incorporan normas a la base normativa. - Se modifican las consideraciones generales. - Se incorporan definiciones. - Se actualizan las actividades. - Se incorpora el registro del evento en el Aplicativo de Mesa de Ayuda como documento que se genera.[2]
02	Base normativa, precisión de actividad y adición de análisis de vulnerabilidades en el Instructivo I-OTI-PA0305-1	- Se agrega una base normativa y se realiza la precisión en la actividad números 1 y 8 sobre la columna de Registro. - Se adiciona el ítem 2.4 de Análisis de Vulnerabilidad en el Instructivo I-OTI-PA0305-1 "Instructivo de monitoreo y seguridad informática[3]".
03	***Objetivo, Alcance, Base Normativa, Actividades, Anexos del procedimiento***	- ***Precisiones de redacción en el objetivo, alcance, base normativa y consideraciones generales.*** - ***Se adecúa el versionamiento del instructivo a la versión del procedimiento[4].***

OBJETIVO	***Establecer las actividades para*** mantener la seguridad de la infraestructura tecnológica del OEFA.
ALCANCE	***El presente*** procedimiento es de aplicación obligatoria de la Oficina de Tecnologías de la Información. Comprende desde la revisión de la alerta de seguridad hasta el registro del control implementado.
RESPONSABLE DEL PROCEDIMIENTO	Jefe/a de la Oficina de Tecnologías de la Información.
BASE NORMATIVA	- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado. - Decreto de Urgencia N° 007-2020-PCM, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento. - Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. - Decreto Supremo N° 030-2002-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado. - Decreto Supremo N° 004-2013-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública. - Decreto Supremo N° 013-2017-MINAM, Decreto Supremo que aprueba el Reglamento de Organización y Funciones del OEFA. - Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo. - ***Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.*** - 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.

[1] Aprobado mediante Resolución de Gerencia General N° 075-2019-OEFA/GEG de fecha 31 de diciembre de 2019.

[2] Aprobado mediante Resolución de Gerencia General N° 051-2021-OEFA/GEG de fecha 09 de junio de 2021.

[3] Modificado mediante la Resolución de Gerencia General N° 0063-2022-OEFA/GEG de fecha 26 de mayo de 2022.

[4] ***Modificado mediante la Resolución de Gerencia General N° 00114-2022-OEFA/GEG de fecha 22 de diciembre de 2022.***

	- Resolución Ministerial N° 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica *vida del software. 3a Edición"*, en todas las entidades integrantes del Sistema Nacional de Informática. - Resolución de Presidencia del Consejo Directivo N° 00020-2022-OEFA/PCD, que aprueba la designación y funciones del Oficial de Seguridad y Confianza Digital del OEFA. - Resolución de Gerencia General N° 051-2020-OEFA/GEG, que aprueba las *"Políticas Específicas de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA"*, vinculadas a la implementación 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"*, aprobada por la Resolución Ministerial N° 004-2016-PCM, modificada por las Resoluciones Ministeriales números 166-2017-PCM y 087-2019-PCM. Las referidas normas incluyen sus modificatorias.
CONSIDERACIONES GENERALES	Las alertas de seguridad informática se generan: - De manera automática por el software de monitoreo disponible; y, - Por los contratistas de servicios de infraestructura con los que cuenta el OEFA. Se atienden las alertas clasificadas como *"críticas"* en el presente procedimiento. ***Se considera toda alerta crítica cuando afecta la normal operación de la Entidad.*** Los tipos de controles a implementar pueden ser: Análisis continuo y eliminación de vulnerabilidades, protección anti-malware, configuraciones seguras para dispositivos de red como firewalls, routers y switches, limitación y control de los puertos de red, protocolos y servicios, entre otros que se consideren pertinentes. Los tipos de riesgo de ciberseguridad a considerar pueden ser: Ransomware, phishing, redes sociales, vishing, entre otros.
DEFINICIONES	- **Alerta crítica:** Ataque importante que se está produciendo y afecta de manera directa a la infraestructura tecnológica de la Entidad. - **Antivirus:** Software que está en condiciones de buscar y eliminar virus en un sistema informático. - **Aplicativo de mesa de ayuda:** Aplicativo informático que permite el registro y seguimiento de las solicitudes de servicios de tecnologías de la información. - **Ciberseguridad:** Práctica a implementar para proteger la información y prevenir o detectar los ataques cibernéticos a los que está expuesto los sistemas electrónicos, las redes y los datos de ataques maliciosos. Se subdivide en categorías tales como: seguridad de red, seguridad de las aplicaciones, seguridad de la información, seguridad operativa, recuperación ante desastres y la continuidad de operación. - **Control automático:** Gestión automática de un control de seguridad informática la cual implica que la operación, monitorización y revisión del mismo se realizan de forma automática, mediante sistemas informáticos o herramientas de hardware; sin que se produzca intervención humana en la realización de estas acciones. - **Firewall:** Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad. - **Infraestructura:** Conjunto de dispositivos físicos y aplicaciones de software que se requieren para operar toda la Entidad. - **Seguridad informática:** Área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional. Conocida también como ciberseguridad o seguridad de tecnologías de la información. - **Software de monitoreo:** Aplicativo que permite identificar en tiempo real qué incidencias se están produciendo en la red, infraestructura y en el código, de manera automatizada. - **Usuario/a:** Servidor/a civil, contratista, tercero/a seleccionado/a practicante pre profesional, practicante profesional y secigrista, que tenga vínculo laboral o contractual con la Entidad; o, se encuentre en alguna modalidad formativa, según corresponda; y, use habitualmente el hardware y software brindados por el OEFA. - **Virus:** Programas que se alojan en la memoria de un ordenador (computadora) con el objetivo de dañar datos o de alterar el normal funcionamiento del equipo
SIGLAS	- OTI: Oficina de Tecnologías de la Información - TI: Tecnologías de la información

REQUISITOS PARA INICIAR EL PROCEDIMIENTO	
Descripción del requisito	**Fuente**
Solicitud de atención de servicios de TI o alerta	Áreas usuarias

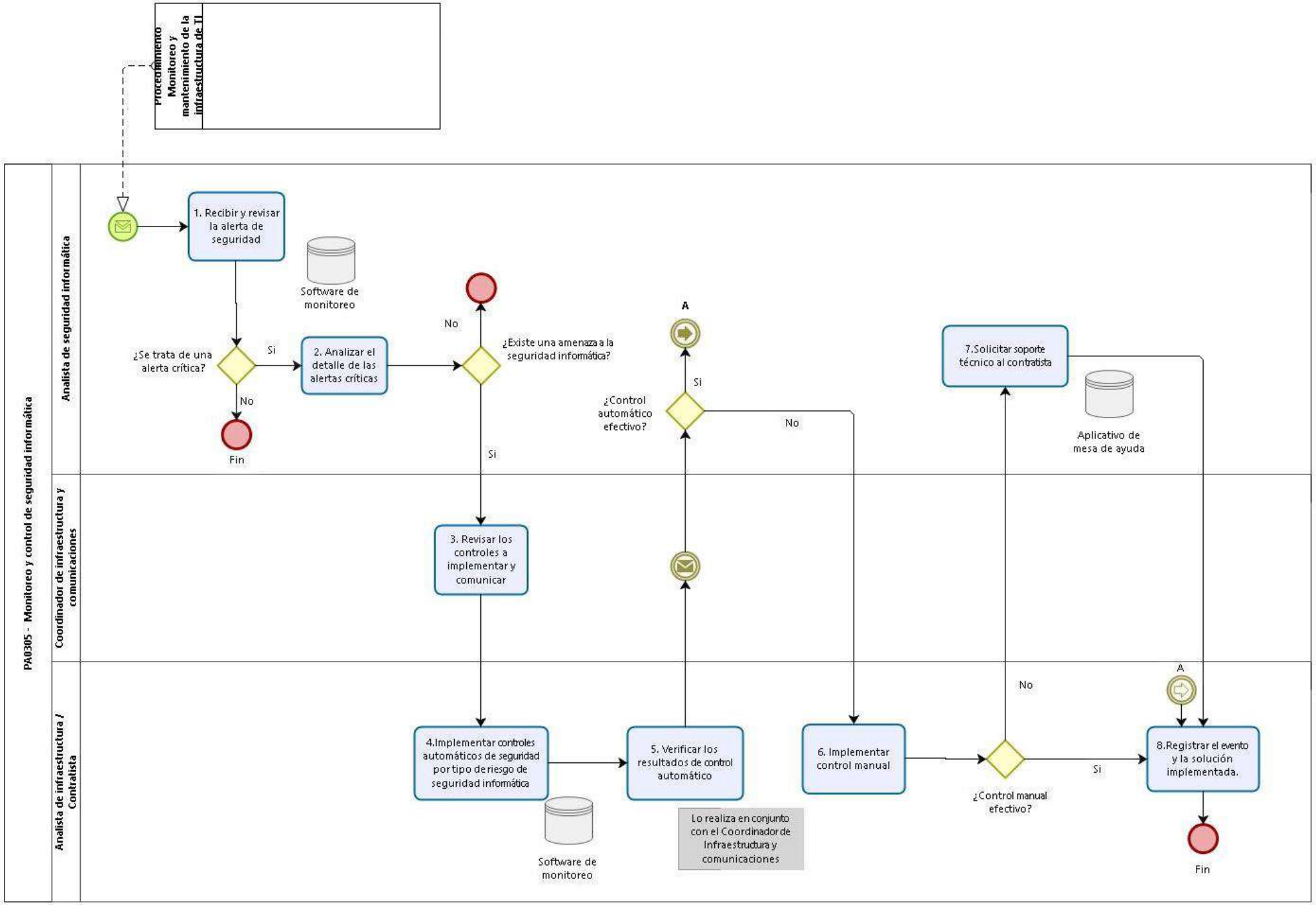
ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
1	Recibir y revisar la alerta de seguridad	Recibe mediante correo institucional, la solicitud de atención de servicios de TI o alerta de seguridad. En ambos casos se revisa las alertas emitidas por el software de monitoreo o por los contratistas de servicios de infraestructura, conforme al I-OTI-PA0305-1 *"Instructivo de Monitoreo y Control de Seguridad Informática".* **¿Se trata de una alerta crítica?** **Sí:** Va a la actividad N° 2. **No: Fin de procedimiento.** *Nota:* *La revisión de los visores de las alertas de seguridad**,** se realizan de manera permanente.*	Correo institucional	Analista de seguridad informática	OTI
2	Analizar el detalle de las alertas críticas	Analiza el detalle de las alertas críticas emitidas por el software de monitoreo. **¿Existe una amenaza a la seguridad informática?** **Sí:** Va la actividad N° 3. **No: Fin de procedimiento.** **Plazo:** En el día hábil de identificada la alerta crítica.	-	Analista de seguridad informática	OTI
3	Revisar los controles a implementar y comunicar	Revisa las amenazas y controles a implementar. *Nota:* *Si la alerta crítica proviene de un ataque de ciberseguridad, se realiza la comunicación, mediante correo institucional, a el/la Jefe/a de la OTI y se coordina la comunicación del control a los/as usuario/as.*	Correo institucional	Coordinador/a de infraestructura y comunicaciones	OTI
4	Implementar controles automáticos de seguridad por tipo de riesgo de seguridad informática	Implementa controles automáticos de seguridad informática de acuerdo con el tipo de riesgo de seguridad informática identificado. **Plazo:** En el día hábil de identificada la alerta crítica.	-	Analista de infraestructura / Contratista	OTI
5	Verificar los resultados de control automático	Verifica el resultado de la implementación del control automático (antivirus, firewall u otro) y comunica**,** mediante	Correo institucional	Analista infraestructura	OTI

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
		correo institucional, a el/la Coordinador/a de Infraestructura y comunicaciones sobre las acciones a implementar. **¿El control automático es efectivo?** **Sí:** Va a la actividad N° 8. **No:** Va a la actividad N° 6. *Nota:* *Cada control automático tiene un tiempo variable de aplicación, proporcional a su complejidad.*			
6	Implementar control manual	Implementa un control manual para lo cual investiga las distintas alternativas de solución para la atención de la alerta crítica. **¿El control manual es efectivo?** **Sí:** Va a la actividad N° 8. **No**: Va a la actividad N° 7. **Plazo:** A los dos (2) días hábiles de verificado que el control automático no fue efectivo. *Nota:* *Dependiendo del nivel de complejidad del control manual a implementarse, el plazo podría extenderse.*	-	Analista infraestructura / Contratista	OTI
7	Solicitar soporte técnico al contratista	Solicita soporte técnico al contratista mediante correo institucional.	Correo institucional	Analista de Seguridad Informática	OTI
8	Registrar el evento y la solución implementada	Realiza el registro del evento y la solución implementada en el aplicativo de mesa de ayuda. **Plazo:** Hasta un (1) día hábil luego de implementada la solución. **Fin del procedimiento.**	Aplicativo de mesa de ayuda	Analista de infraestructura / Contratista	OTI

DOCUMENTOS QUE SE GENERAN:
Reporte de Alerta de monitoreo de Software. Registro del evento en el Aplicativo de mesa de ayuda.

ANEXO DEL PROCEDIMIENTO:
Instructivo I-OTI-PA0305-1: *"Instructivo de monitoreo y control de seguridad informática"*.

PROCESO RELACIONADO
PA03 - Tecnologías de la información.



Instructivo de monitoreo y control de seguridad informática

I. OBJETIVO

Establecer las tareas para facilitar el correcto funcionamiento de las operaciones de tecnologías de la información a nivel de seguridad y control considerando la atención de tickets[1] y el monitoreo de la infraestructura, a través de las disposiciones específicas.

II. INSTRUCCIONES

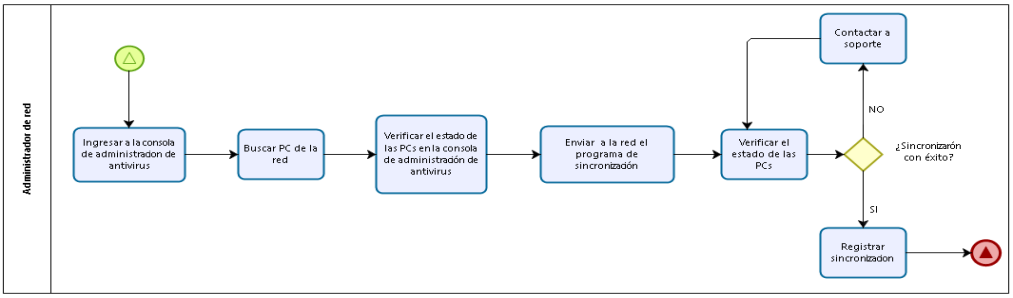
A. Para la administración del antivirus, se observa lo siguiente:

2.1 Configuración del agente de red

La sincronización es una tarea programada mediante la cual, el administrador de redes lanza la sincronización del servidor informático a todas las computadoras conectadas en la red de la Entidad, para ello el administrador del antivirus desarrolla las siguientes acciones:

a) Ingresa a la consola de administración de antivirus y realiza la búsqueda de las PC en la red.
b) Verifica el estado de las PC en la consola de administración de antivirus.
c) Envía el programa de sincronización todas las PC.
d) Verifica el estado de las PC.
e) Si ocurre un problema en la sincronización se contacta con el área de soporte.
f) Si la sincronización fue un éxito, se actualiza el registro de sincronización.

Para lo cual, se presenta el siguiente flujograma:



2.2 Monitoreo de virus

El monitoreo de existencia de virus es una tarea programada para la cual se elabora una política[2] en el antivirus, mediante la cual se califica a las PC según la cantidad de virus que identifican en la PC para colocarla luego en una lista donde se bloquea los puertos de la PC para evitar el contagio con virus informáticos y propagarlos en la red, para lo cual el administrador de red desarrollara las siguientes actividades:

a) Ingresa a la consola de administración del antivirus y elabora la política de antivirus para envió de PC a zona de bloqueo de USB.

---

1 Un ticket básicamente es cualquier tipo de consultas, sugerencias o mejoras al producto adquirido, reclamos, pedidos o asesoramiento que como usuario de alguno de nuestros productos o servicios se pueda realizar por la mesa de ayuda.

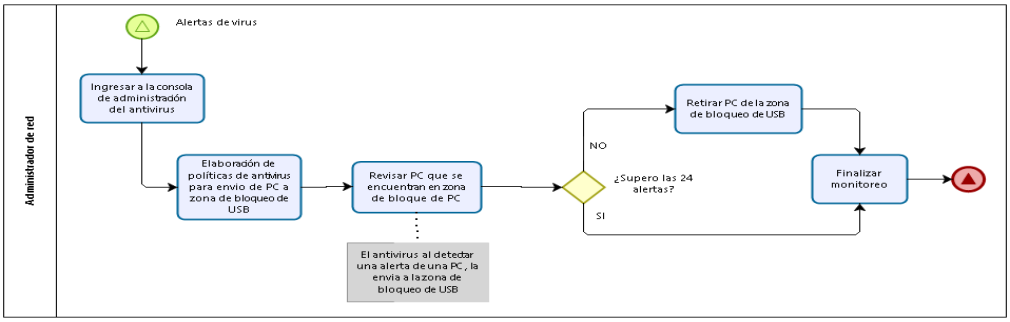
2 Se refiere a la configuración de las bases de datos para la generación de los tipos y frecuencias de los backup.

b) Revisar la zona de bloqueo de PC y revisar las cantidades de alertas de virus.

- La política del antivirus clasifica a la PC en zona de bloqueo de puertos a la primera alerta.
- Si una PC supera las veinticuatro (24) alertas debe de mantenerse en la zona de bloqueo.

c) Retirar la PC de la zona de bloqueo, si ésta no supera las veinticuatro (24) alertas y finalizar el monitoreo.

Respecto de ello, se presenta el siguiente flujograma:

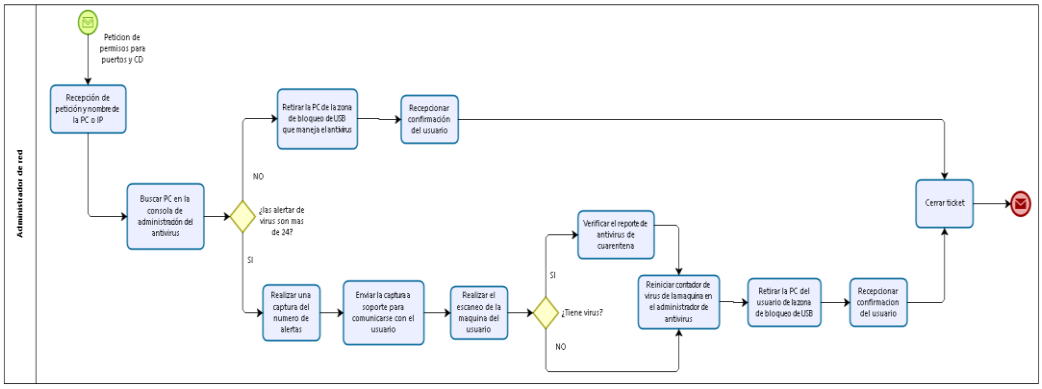


2.3 Permiso de acceso a puertos USB y CD

La atención de acceso a puertos USB y CD se inicia con la recepción de un ticket de un/a usuario/a que tiene los puertos bloqueados por haber reportado una alerta de virus, para ello se desarrollan las siguientes acciones:

a) Se recibe el ticket o solicitud, en la cual se especifica el nombre o la IP (Internet Protocol) de la PC (Personal Computer).
b) Buscar la PC mediante la consola de administración del antivirus.
c) Se evalúa la cantidad de alertas reportadas por la máquina si son menos de 24 se retira la PC de la zona de puertos bloqueados.
d) Se informa al usuario y se cierra el ticket.
e) En caso de haber pasado el número de alertas, se realiza la captura del informe del antivirus.
f) Se envía la captura a soporte para que comunique a el/la usuario/a.
g) Se realiza un escaneo de la PC de el/la usuario/a.
h) Proceder a eliminar los virus.
i) Reiniciar el contador.
j) Se retira la PC del usuario de la zona de bloqueo de puertos.
k) Se informa al usuario y se cierra el ticket.

Para lo cual, se presenta el siguiente flujograma:



2.4 Respecto al Análisis de vulnerabilidad:

El/La Analista de Seguridad informática determina el alcance del servicio y se contrata a una empresa especializada en pruebas de Ethical Hacking a nivel de la infraestructura, web y aplicaciones. Luego que el servicio emita el informe de vulnerabilidades encontradas se realiza lo siguiente:

- Se convoca a una reunión para mostrar las vulnerabilidades encontradas en la cual participan los/as responsables del levantamiento de observaciones.
- Se muestra el reporte y evidencias de las observaciones encontradas y los/as responsables comunican el tiempo de levantamiento de dichas observaciones.
- Se realiza un seguimiento trimestral para verificar si las recomendaciones realizadas por los contratistas han sido implementadas.
- Si los/as responsables indican que las recomendaciones fueron absueltas, se procede a contratar un servicio de Ethical Hacking para el re test, es decir se vuelve a realizar las pruebas para verificar si los controles implementados por los/as responsables de cada vulnerabilidad han sido levantados.
- Una vez que esto haya sido validado se procede a dar por implementada la recomendación.