1. OBJETIVO

Establecer el procedimiento técnico para verificar, controlar, actualizar y monitorear la plataforma de antivirus de la Caja de Vivienda Popular; detectando y eliminando todo posible virus informático o posibles amenazas de virus que busquen generar caos, sustraer información o causar daños críticos a la seguridad de la información de la entidad.

2. ALCANCE

Inicia con la verificación de la existencia de solución de antivirus en la entidad junto con la adquisición de este software si es requerido, a fin de establecer las políticas operacionales a nivel de comportamiento del antivirus en la Caja de Vivienda Popular hasta la puesta en marcha de esta solución en la red de datos y en cada equipo de cómputo. En caso de que la infraestructura tecnológica se encuentre administrada mediante Hosting en la nube por parte de un tercero, este será el responsable de la administración de la solución de antivirus hasta su soporte y monitoreo.

Nota: Al existir hosting de servicios tecnológicos en la entidad, la solución de software de antivirus no debe ser necesariamente la misma con la cual cuenta la CVP pero si debe cumplir con los estándares de seguridad que se requieran para la protección de estos servicios.

3. RESPONSABLES

Jefe de área de la Oficina de Tecnologia de la información y las comunicaciones de la Caja de Vivienda Popular – CVP es responsable de la actualización y/o modificación de este procedimiento.

Adicional, la autorización para la administración y monitoreo del software de antivirus de la entidad, será asignada al profesional universitario y/o contratista de la Oficina de Tecnología de la Información y las comunicaciones.

4. GENERALIDADES O POLÍTICAS OPERACIONALES

- Para garantizar la confidencialidad, integridad y disponibilidad de la información todo computador/servidor de pertenencia a la CVP y que requiera acceder a la red de datos de la entidad; debe contar con el software de antivirus contratado instalado y en ejecución en su última versión de actualización de ser posible, de lo contrario se restringirá el acceso en su conexión y operatividad.

- Los usuarios deben cumplir con todas las restricciones que la plataforma antivirus tiene configurada para evitar la propagación de virus informáticos como lo son la instalación de software de terceros desconocidos y no aprobados por la Oficina TIC, lo anterior siguiendo la documentación de la política 208-TIC-Mn-07 Política de Seguridad de la Información.

- Las actualizaciones generadas por el fabricante de antivirus serán distribuidas a los equipos de la CVP desde la consola de administración del antivirus a fin de garantizar control y verificación del proceso de actualización y protección en tiempo real de los equipos de cómputo de la entidad.

5. DEFINICIONES Y SIGLAS

- **Amenaza informática:** Es una acción que surge a partir de vulnerabilidades en sistemas de información, equipos tecnológicos o redes de datos, que cuenta con la capacidad de afectar y transgredir la seguridad de la información; como consecuencia sufrir pérdidas irrecuperables en los datos de una entidad.

- **Base de datos de firmas:** Consiste en un conjunto de datos en donde se almacenan fragmentos o muestras del comportamiento de los virus o malwares, permitiendo identificarlos, definirlos y reaccionar frente a una intrusión de seguridad.

- **Consola de administración:** Interfaz que provee acceso a las funciones del software antivirus.

- **CVP:** Caja de la Vivienda Popular.

- **Endpoint:** Corresponde a todo dispositivo tecnológico que haga parte final de una red que cuenta con un software de antivirus, es decir elementos tecnológicos que se comunican a través de una red de datos a la que se encuentren

conectados como (Tablet, computadores de mesa, portátiles, dispositivos móviles etc); y que a su vez representan un riesgo de vulnerabilidad importante en favor de los ciberdelincuentes que buscan vulnerar la seguridad de un sistema.

- **Gateway de internet:** Equipo que permite la conectividad con la internet aplicando políticas de uso.

- **Grupo de política de antivirus:** Reglas o parámetros establecidos en la administración principal de la consola antivirus hacia cada uno de los endpoint o dispositivos de usuario final; con el fin de controlar y delimitar la ejecución de aplicaciones, herramientas y apertura de archivos a fin de garantizar la seguridad de la información.

- **Logs de registro de eventos**: Son archivos que registran actividades y movimientos de un programa. Estos archivos son simplemente archivos de texto. Su misión es la de registrar todos los sucesos.

- **Malware:** Es un software malicioso desarrollado por ciberdelincuentes con intención de robar datos para su beneficio, sembrar caos, o exponer información vulnerable de una entidad; estos pueden identificarse como (Troyanos, gusanos, ransomware entre otros) y a su vez pueden llegar a contar con la capacidad de afectar a los demás dispositivos conectados y comunicados en la misma red.

- **Parche de actualización:** Un parche consta de cambios que se aplican a una aplicación de software, para corregir errores o mejorar su funcionalidad.

- **Software licenciado:** Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario del programa informático (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

- **Software de Antivirus:** Programa o herramienta encargado de detectar, controlar y mantener la seguridad en los equipos de cómputo o redes de datos que sean vulnerables a amenazas de software malicioso o perjudicial, en búsqueda de afectar el servicio tecnológico o hurto de información sensible; cuyo objetivo se enfoca en mitigar y prevenir los posibles impactos negativos en una entidad a nivel de ciberseguridad y los diferentes servicios que este preste.

- **Spam:** Conocido coloquialmente como correos “basura”, el spam es un mensaje no solicitado que se entrega en su mayoría de veces mediante correo electrónico de mensajería (Gmail, Outlook entre otros). No obstante, también puede ser empleado desde cualquier herramienta tecnológica como servicios de mensajería instantánea o redes sociales donde su imagen de presentación se realiza mediante avisos informativos o publicitarios que buscan captar la atención del destinatario.

- **Vulnerabilidad:** Conocida también como agujeros de seguridad, esta consiste en una debilidad o fallo en un sistema operativo, equipos de infraestructura de red o sistemas de información que puedan llegar a comprometer la integridad, disponibilidad o confidencialidad de la seguridad de la información.

6. DESCRIPCIÓN DE ACTIVIDADES

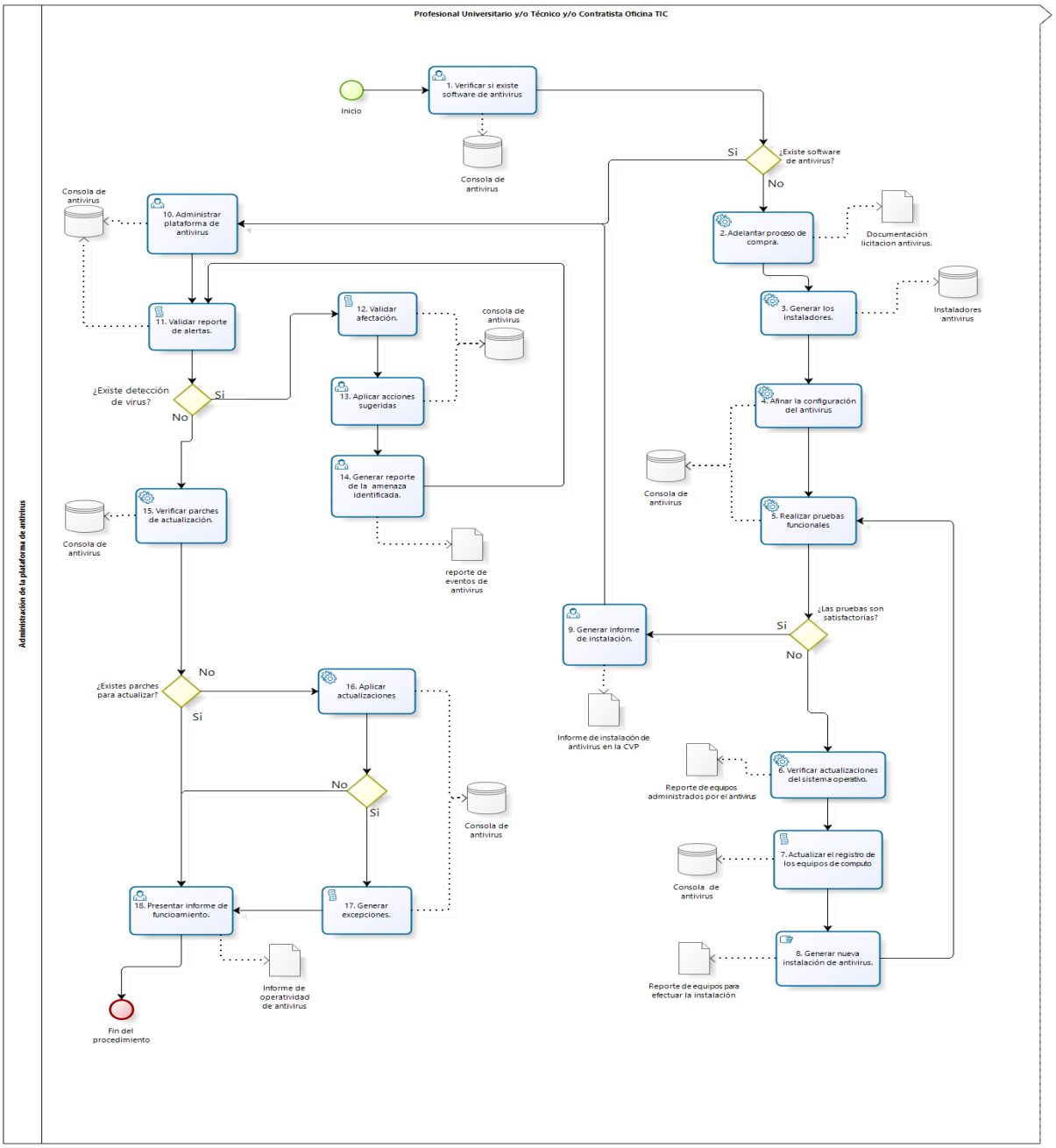
N°	Actividad y Descripción	Responsable	Registros
1	Verificar si existe software de antivirus ¿Existe software de antivirus instalado en la entidad? Si: ir actividad No. 9 No: Ir a actividad No.2	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC y/o Jefe de Oficina TIC	Software de antivirus
2	Adelantar proceso de compra de software de antivirus para la entidad.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC y/o Jefe de Oficina TIC	Documentación de licitación de software de antivirus Secop II
3	Generar los instaladores correspondientes para los EndPoint o equipos de cómputo de la entidad desde la consola de antivirus para que sean instalados en su totalidad.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Instalador software de antivirus
4	Afinar la configuración del antivirus de acuerdo a las necesidades de protección de la Caja de la Vivienda Popular.	Profesional Universitario y/o Técnico y/o	Consola de administración del antivirus

N°	Actividad y Descripción	Responsable	Registros
		Contratista Oficina TIC	
5	Realizar pruebas funcionales durante cinco días anteriores a la instalación del software de antivirus, conforme a las políticas creadas e implementadas en la consola de antivirus junto con el log de eventos de los equipos de cómputo a los cuales les fue implementada las políticas. ¿Las pruebas de funcionamiento de la plataforma de antivirus son satisfactorias? Si: Continuar en la actividad 9. No: Continuar en la actividad 6.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus. Logs de eventos de la consola de administración
6	Verificar actualizaciones del sistema operativo para las instalaciones de antivirus efectuadas en los equipos de cómputo de la entidad.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Reporte de equipos administrados por la consola de antivirus
7	Actualizar el registro de los equipos de cómputo en la consola de administración.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus
8	Generar nueva instalación del antivirus en el equipo con las fallas reportadas. Volver a la actividad 5 a fin de generar las pruebas funcionales correspondientes a las instalaciones realizadas en base a los errores reportados.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Reporte de equipos de cómputo para efectuar la instalación de antivirus.
9	Generar informe de instalación desde la plataforma de antivirus solicitando al proveedor dicho documento acorde a las instalaciones, cada vez que se realiza la adquisición del software de antivirus.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Informe de instalación de antivirus en la CVP
10	Administrar el funcionamiento de la plataforma de antivirus y los endpoint instalados.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus.

N°	Actividad y Descripción	Responsable	Registros
11	Validar las alertas de manera diaria reportadas por la plataforma de antivirus a fin de identificar detección de software malicioso. ¿Existe detección de virus o ataque informático? Si: Pasar a actividad 11 No: Pasar a actividad 15	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus.
12	Validar la afectación de la infraestructura tecnológica según la amenaza identificada.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus.
13	Aplicar las acciones sugeridas del fabricante de antivirus a fin de mitigar la amenaza detectada.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus.
14	Generar un reporte de la amenaza identificada y los archivos afectados para comunicar al Jefe Oficina TIC y el proveedor de antivirus. Volver a la actividad No.11 para identificar el centro de alertas de antivirus después de haber aplicado las acciones sugeridas por la herramienta.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Reporte de eventos de antivirus
15	Verificar los parches de actualización del software de antivirus emitidos por el fabricante. ¿Existen actualizaciones o parches para actualizar? Si: continúe actividad 16. No: continúe actividad 18.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus
16	Aplicar las actualizaciones de base de virus en la consola de administración del antivirus y los endpoint registrados de acuerdo con la periodicidad en la que el fabricante realice sus respectivas	Profesional Universitario y/o Técnico y/o	Consola de administración del antivirus.

N°	Actividad y Descripción	Responsable	Registros
	actualizaciones de base de firmas. ¿La actualización fue rechazada? Si: continúe actividad 17. No: continúe actividad 18.	Contratista Oficina TIC	
17	Generar una excepción del parche actualizado en la consola de administración de antivirus.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Consola de administración del antivirus.
18	Presentar informe mensual del estado actual de funcionamiento de la consola de antivirus y los endpoint para garantizar seguridad sobre los equipos de la entidad.	Profesional Universitario y/o Técnico y/o Contratista Oficina TIC	Informe de operatividad de antivirus
	Fin del procedimiento		

7. DIAGRAMA DE FLUJO



Ver Diagrama de Flujo Anexo en la Carpeta de Calidad de la Entidad

8. PUNTOS DE CONTROL

N° Actividad	Actividad	¿Qué y cómo se controla?	¿Con qué frecuencia?	¿Quién lo controla?
10	Validar las alertas reportadas por la plataforma de antivirus.	Confidencialidad, integridad, disponibilidad de la información. Prevención y control en la apertura y o ejecución de software malicioso.	Diariamente	Profesional Universitario y/o técnico y/o Especializado - Contratista Oficina TIC
12	Aplicar las acciones sugeridas del fabricante de antivirus a fin de mitigar la amenaza detectada.		Según la amenaza que se identifique.	
14	Verificar los parches de actualización del software de antivirus emitidos por el fabricante.		De acuerdo con la frecuencia de publicación de actualizaciones por parte del proveedor.	
15	Aplicar las actualizaciones de base de virus en la consola de administración del antivirus y los endpoint registrados de acuerdo con la periodicidad en la que el fabricante realice sus respectivas actualizaciones de base de firmas.			
17	Presentar informe del estado actual de funcionamiento de la consola de antivirus y los endpoint para garantizar seguridad sobre los equipos de la entidad.		Mensual	

9. DOCUMENTOS RELACIONADOS

9.1 Normograma

- Ver Normograma

9.2 Documentos Internos

- Ver Listado Maestro de Información Documentada o Listado Maestro de Documentos

9.3 Formatos Asociados

- No Aplica

9.4 Documentos Externos

Nombre del Documento	Fecha de publicación o versión del documento	Entidad que lo emite	Ubicación
N/A	N/A	N/A	N/A

10. ANEXOS

- No Aplica

11. CONTROL DE CAMBIOS

Versión	Fecha Aprobación (dd-mm-aaaa)	Cambios	Revisó Nombre y Cargo Líder del Proceso
1	05-11-2015	Documento inicial	Martha Liliana González Directora de Gestión Corporativa y CID
2	02-12-2021	Actualización del procedimiento en la plantilla vigente - 208-PLA-Ft-65 Procedimiento V4. Se realizan ajustes en los siguientes ítems: • Objetivo. • Alcance. • Responsables. • Políticas operacionales. • Definiciones y Siglas. • Descripción de actividades. • Elaboración diagrama de procesos haciendo uso de la herramienta Bizagi Process Modeler. • Puntos de Control.	Leydy Yohana Pineda Afanador – Jefe Oficina TIC

12. APROBACIÓN

ELABORADO	REVISADO	APROBADO
Nombre: Fabian David Rojas Castiblanco **Cargo:** Contratista **Fecha:** 29 de noviembre de 2021	**Nombre:** Leydy Yohana Pineda Afanador **Cargo:** Jefe Oficina TIC **Fecha:** 26-11-2021	**Nombre:** Catalina Nagy Patiño **Cargo:** Jefe Oficina Asesora de Planeación **Fecha:** 02-12-2021