1. OBJETO:

Establecer las actividades para prevenir, detectar, corregir y eliminar la presencia de software malicioso en los componentes de tecnología de la Unidad Administrativa Especial de Servicios Públicos garantizando la seguridad de la información.

2. ALCANCE:

Inicia con la instalación, verificación, actualización del antivirus y finaliza con el informe de gestión.

Este procedimiento aplica para los siguientes ambientes tecnológicos:

- Servidores, físicos, virtuales y en la nube, que hacen parte de la plataforma tecnológica de la UAESP con sistemas operativos soportados por la herramienta de antivirus.
- Equipos de cómputo portátiles y de escritorio de la Entidad con sistemas operativos soportados por la herramienta de antivirus.
- Dispositivos móviles de la Entidad con sistemas operativos soportados por la herramienta de antivirus.

3. DEFINICIONES:

Activo de información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización y por lo tanto se debe proteger.

Antivirus: Software que detecta, limpia o elimina los virus informáticos existentes en el computador.

EndPoint: El termino hace referencia a un dispositivo informático remoto que se comunica con una red a la que está conectado. Los ejemplos de Enpoint incluyen: ordenadores de escritorio, portátiles, tablets, servidores, estaciones de trabajo, entre otros.

Log o Logs: Registro o Registros. Termino técnico usado para los datos que se genera en los sistemas (Servidores, Aplicaciones, Programas, etc) en forma de trazas textuales en el que constan cronológicamente los acontecimientos que afectan a un sistema o el conjunto de cambios que generan.

Virus Informático: Es un programa o un segmento de código creado con el objetivo de causar daños en los computadores, el cual puede ocasionar graves consecuencias para el computador que lo almacena**.**

4. NORMATIVA:

NUMERO	DESCRIPCIÓN
Decreto 415 del 7 de marzo de 2016	Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones

5. DESCRIPCIÓN DE ACTIVIDADES:

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
1	**Realizar la instalación o Actualización** Instala y configura la plataforma de Antivirus, o las actualizaciones críticas, de acuerdo con el servicio (Servidores, mail, PC, entre otros).	Acuerdos de Nivel de Servicio o el Contrato	Técnico / Profesional Universitario / Contratista Oficina TIC o Fabricante o Proveedor	Log de eventos en la consola de antivirus o Informe del fabricante
2	**Realizar las pruebas** Realiza las pruebas, verifica el funcionamiento normal de la plataforma y los agentes de los EndPoint y realiza los ajustes necesarios.		Técnico / Profesional Universitario / Contratista Oficina TIC	Log de eventos en la consola de antivirus. Bitácora de gestión antivirus.
3	**Verificar Actualizaciones** Verifica semanalmente las actualizaciones del software a través de la plataforma de gestión.	Log de eventos en la consola.	Técnico / Profesional Universitario / Contratista Oficina TIC	Log de eventos en consola antivirus
	¿El Equipo o dispositivo se actualizó? Si: Continúa con la actividad No 5. No: Continúa con la actividad No 4.			
4	**Actualizar el dispositivo** Realiza la actualización de forma manual en el dispositivo (Servidor, PC, Dispositivo Móvil, entre otros) y pasar a la actividad 8.		Técnico / Profesional Universitario / Contratista Oficina TIC	Log de eventos en la consola antivirus
5	**Realizar el monitoreo**	Alertas generadas por	Técnico / Profesional	Log de eventos de consola antivirus

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	Realiza el monitoreo y revisa las alertas generadas de amenazas y funcionamiento de la plataforma de antivirus.	la consola / Logs de eventos.	Universitario / Contratista Oficina TIC	
	¿Se detectó una amenaza? Si: Continúa con la actividad No 6. No: Continúa con la actividad No 11			
6	**Eliminar Amenaza** La plataforma de Antivirus neutraliza o elimina de forma automática la amenaza. Si la amenaza no es neutralizada o eliminada de forma automática pasa a la actividad No 7. Si la amenaza es neutralizada o eliminada de forma automática y hubo afectación a algún activo de información, pasar a la actividad No 10. Si la amenaza es neutralizada o eliminada de forma automática y no hubo afectación a algún activo de información, pasar a la actividad No 11.		Plataforma y EndPoint del Antivirus	Log de eventos de consola antivirus
7	**Eliminar Amenaza de forma Manual** Neutraliza o elimina de forma manual la amenaza en el dispositivo afectado.		Técnico / Profesional Universitario / Contratista Oficina TIC	Bitácora de gestión antivirus.

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
8	**Reportar al fabricante** Reporta al fabricante la amenaza o malfuncionamiento de la plataforma de antivirus por correo electrónico o en los canales dispuesto para ello.	Contrato / Acuerdos de Nivel de Servicio	Técnico / Profesional Universitario / Contratista Oficina TIC	Correo electrónico
9	**Recibir la actualización del fabricante** Recibe, por parte del fabricante del software, la respectiva actualización del antivirus o aplica el procedimiento recomendado para la eliminación de la amenaza.	Procedimientos o lineamientos dados por el fabricante.	Técnico / Profesional Universitario / Contratista Oficina TIC	Actualizaciones o procedimiento del fabricante.
	¿Algún activo de información fue afectado? Si: Continúa con la actividad No 10. No: Continúa con la actividad No 11.			
10	**Activar el procedimiento reporte de incidentes de seguridad de la información** Reportar a la mesa de ayuda el caso o incidente en los canales establecidos en el procedimiento reporte de incidentes de seguridad de la información. Continúa con el procedimiento GTI-PC-16 Reporte de incidentes de seguridad de la información		Técnico / Profesional Universitario / Contratista Oficina TIC	Reporte Mesa de Ayuda
11	**Alimentar Bitácora** Alimenta la bitácora de		Técnico / Profesional Universitario /	Bitácora de gestión de antivirus actualizada.

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	gestión de antivirus.		Contratista Oficina TIC	

6. CONTROL DE CAMBIOS:

Versión	Fecha	Descripción de la modificación
01	30/11/2015	Adopción del procedimiento
02	06/08/2021	Se actualiza el Procedimiento en su formato. Se definen las actividades de instalación inicial por parte del fabricante y las pruebas de funcionamiento. Se define las actividades de actualización y eliminación de forma manual cuando no se hacen automáticamente. Se articula la gestión de incidentes mediante la definición de la actividad 10.

7. AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Sebastián Perdomo Mendez	Profesional Universitario Oficina TIC	
	Fabian Andres Lozano Aguilar	Contratista – Oficina TIC	
	Rubén Esteban Buitrago Daza	Contratista – Oficina TIC	
	Osbaldo Cortes Lozano	Profesional Universitario Oficina TIC	
Revisó	Cesar Mauricio Beltrán López	Jefe Oficina de Tecnologías de Información y las Comunicaciones	César Mauricio Beltrán López Firmado digitalmente por César Mauricio Beltrán López Fecha: 2021.08.03 15:09:45 -05'00'
	Luz Mary Palacios Castillo	Profesional Oficina Asesora de Planeación	
Aprobó	Francisco José Ayala Sanmigel	Jefe Oficina Asesora de Planeación	