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 antimalware y finaliza con el informe de gestión.

Este procedimiento aplica para los siguientes ambientes tecnológicos de la entidad:

- 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 antimalware.
- Equipos de cómputo portátiles y de escritorio de la Entidad con sistemas operativos soportados por la herramienta de antimalware.
- Dispositivos móviles de la Entidad con sistemas operativos soportados por la herramienta de antimalware.

3. DEFINICIONES:

Amenaza: Cualquier evento o acción con el potencial de explotar vulnerabilidades y causar daño a los sistemas informáticos, la información o los servicios, como la introducción de malware, accesos no autorizados o ataques dirigidos.

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.

Evento de seguridad: Ocurrencia o cambio identificado en un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

Firma del malware: Patrón específico de código o comportamiento utilizado para identificar y detectar un software malicioso en un sistema o red.

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.

Malware: Es cualquier tipo de programa o código diseñado para dañar, interrumpir o acceder sin autorización a un sistema, red o dispositivo. Incluye virus, troyanos, gusanos, ransomware, spyware, entre otros.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, hay que considerar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad que también pueden estar involucrados.

4. NORMATIVA:

TABLA 1 NORMATIVA APLICABLE AL PROCEDIMIENTO

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
Resolución 00500 del 10 de marzo del 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

Fuente: Normograma UAESP

5. LNEAMIENTOS DE OPERACIÓN:

No aplica

6. DESCRIPCIÓN DE ACTIVIDADES:

TABLA 2 DESCRIPCIÓN DE ACTIVIDADES

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
1	**Realizar la instalación o Actualización** Instala y configura la plataforma de antimalware, incluyendo los agentes para servidores, dispositivos móviles, endpoint o las actualizaciones críticas, según aplique, de acuerdo con el servicio contratado.	Acuerdos de Nivel de Servicio o Contrato	Técnico / Profesional / Contratista Oficina TIC o Fabricante o Proveedor	Log de eventos en la consola de antimalware 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 / Contratista Oficina TIC O Fabricante o Proveedor	Log de eventos en la consola de antimalware o Informe mensual de gestión de riegos
3	**Verificar Actualizaciones** Verifica semanalmente las	Plataforma de antimalware	Técnico / Profesional /	Log de eventos en

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	actualizaciones de la herramienta antimalware a través de la plataforma de gestión.		Contratista Oficina TIC	consola antimalware
	¿La plataforma o los agentes se encuentran actualizados? Si: Continúa con la actividad No. 5 No: Continúa con la actividad No. 4			
4	**Actualizar la plataforma o el agente** Realiza la actualización a través de la consola de administración, o en caso de ser necesario, de forma manual en los dispositivos (Servidor, PC, Dispositivo Móvil, entre otros).		Técnico / Profesional / Contratista Oficina TIC	Log de eventos en consola antimalware
5	**Realizar el monitoreo** Realiza periódicamente el monitoreo y revisa las alertas generadas de amenazas y funcionamiento de la plataforma de antimalware.	Alertas generadas por la consola / Logs de eventos	Técnico / Profesional / Contratista Oficina TIC	Log de eventos en consola antimalware
	¿Se detectó una amenaza? Si: Continúa con la actividad			

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	No. 6 No: Continúa con la actividad No. 9			
6	**Eliminar Amenaza** Utiliza la plataforma de antimalware para neutralizar o eliminar de forma automática la amenaza.		Plataforma y EndPoint del Antimalware	Log de eventos de consola antimalware
	¿Se neutralizó o eliminó la amenaza de forma automática? Si: Continúa con la actividad No. 9 No: Continúa con la actividad No. 7			
7	**Eliminar Amenaza de forma Manual** Neutraliza o elimina de forma manual la amenaza en el dispositivo afectado. Si se detecta un evento de seguridad con afectación a la seguridad de la información, activar el procedimiento GTI-PC-16 Gestión de incidentes de seguridad de la información.		Técnico / Profesional Universitario / Contratista Oficina TIC	Informe mensual de gestión de riesgos Reporte Mesa de servicios
8	**Actualizar firmas o reportar al fabricante**	Contrato / Acuerdos de	Técnico / Profesional	Informe mensual de

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	Reporta al fabricante la amenaza o firmas del malware por los canales dispuesto para ello, si la plataforma no tiene la opción de reporte o alimentación de firmas.	Nivel de Servicio Correo Electrónico Canales de comunicación del fabricante	Universitario / Contratista Oficina TIC	gestión de riesgos Comunicación oficial
9	**Elaborar Informe Mensual** Elabora informe de gestión de riesgos de la gestión realizada durante el mes correspondiente.		Técnico / Profesional / Contratista Oficina TIC	Informe mensual de gestión de riesgos

Fuente: UAESP

7. CONTROL DE CAMBIOS:

TABLA 3 CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	30/11/2015	Adopción del procedimiento
2	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.
3	04/07/2025	Se ajustó el nombre del procedimiento de “Administración de antivirus” a “Administración de antimalware”. Se ajusta la redacción y lógica en las

Versión	Fecha	Descripción de la modificación
		actividades, se elimina un registro no utilizado llamado “Bitacora” y se cambia por el informe mensual de gestión de riesgos.

Fuente: UAESP

8. AUTORIZACIONES:

TABLA 4 AUTORIZACIONES

	NOMBRE	CARGO	FIRMA
Elaboró	Eduardo Andres Rozo Revelo	Profesional Universitario Oficina TIC	
	Juan Sebastian Perdomo Mendez	Profesional Universitario Oficina TIC	
Revisó	Jorge Alexis Rodriguez Meza	Jefe Oficina TIC	
	Luz Mary Palacios Castillo	Profesional universitario Oficina Asesora de Planeación	
Aprobó	Marcela Toro Pascagaza	Jefe Oficina Asesora de Planeación