POLÍTICAS DE CONTROLES CONTRA MALWARE

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido / Cargo	Firma
Elaborado por:	Ing. Geovanny Meza, Mg. **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: JORGE GEOVANNY MEZA MORALES
	Ing. Darío Braganza **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: DARIO JAVIER BRAGANZA SUAREZ
Revisado y aprobado por:	Ing. Patricio Padrón **Director de Tecnologías de la Información y Comunicación**	Firmado electrónicamente por: NARDO PATRICIO PADRON CORREA

ÍNDICE

1. Notas de Cambio

Versión	Fecha	Detalle de la modificación
1	16/11/2021	Creación de la política

2. Antecedentes

El Esquema Gubernamental de Seguridad de la Información (EGSI), establece una serie de hitos que contemplan la elaboración, implementación y difusión, de políticas, procedimientos, reglamentos, normas y demás instrumentos técnicos, que garanticen el manejo seguro de la información de las instituciones públicas.

El malware así como los virus informáticos en general, son una amenaza latente para la seguridad de la información, es por ello que se requiere establecer políticas que permitan a la institución, mantener controlada dicha amenaza.

3. Alcance

Las políticas aquí descritas son de alcance general; es decir, para todos los servidores, funcionarios, instancias, dependencias, procesos y subprocesos del Secap.

4. Propósito

Establecer políticas de cumplimiento obligatorio para controlar el malware y evitar la infección de los equipos institucionales con dichos programas maliciosos.

5. Definiciones

- **Aplicaciones de software:** Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
- **Antimalware:** Tipo de software, programa o aplicación diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos.
- **Antivirus:** Software o aplicación que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora.
- **Internet:** Red mundial de computadores conectadas entre sí que ofrecen acceso y comparten información a través de un lenguaje común.
- **Intranet:** Red informática interna basada en los estándares de internet.

- **Malware:** Software o aplicación que realiza acciones dañinas a los sistemas informáticos, de forma intencionada y sin el conocimiento del usuario.
- **Red de computadores:** Conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.).
- **Seguridad del sistema:** Conjunto de medidas preventivas y correctivas que permiten resguardar y proteger la información y los sistemas de software que la procesan y almacenan.
- **Servicios:** Conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor del Secap.
- **Servidor/funcionario:** Persona que presta servicios a la Administración o a nombre y por cuenta de esta, como parte de su organización, en virtud de un acto válido y eficaz de investidura, con entera independencia del carácter imperativo, representativo, remunerado, permanente o público de la actividad respectiva.
- **Sistema de software:** Programas informáticos diseñados con el propósito de facilitar a los usuarios la realización de determinadas tareas.
- **Usuario:** Nombre o identificador compuesto por una cadena de caracteres alfanuméricos, que emplea una persona para identificarse en un sistema, equipo o red, previo a ingresar la contraseña.
- **Virus informático:** Software o aplicación que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario, principalmente para lograr fines maliciosos sobre el dispositivo.

6. Políticas

- La Dirección de Tecnologías de la Información y Comunicación a través del área de Gestión de Administración de Servicios, Componentes de TI y Soporte Técnico a Usuarios, implementará una solución antivirus y antimalware institucional, misma que estará instalada en todos los equipos de cómputo institucionales.
- La Dirección de Tecnologías de la Información y Comunicación a través del área de Gestión de Administración de Servicios, Componentes de TI y Soporte Técnico

a Usuarios, es responsable de mantener actualizado el antivirus y antimalware institucional.

- Todo servidor o funcionario del Secap es responsable del correcto uso, manejo y custodia de los equipos y medios extraíbles que se le hayan asignado; así como, la información que crea, disponga y almacene en dichos dispositivos; por lo que, es a la vez responsable de cuidar que los dispositivos asignados, estén libres de malware o cualquier otro tipo de virus informático.
- Todo servidor o funcionario del Secap requerirá a la Dirección de Tecnologías de la Información y Comunicación, la instalación o actualización del antivirus y antimalware en su equipo institucional debidamente asignado, en caso de que no lo tenga instalado o actualizado.
- Todo servidor o funcionario del Secap, previo a usar un dispositivo de almacenamiento extraíble en los equipos institucionales, debe hacer una revisión del dispositivo utilizando el antivirus y antimalware actualizado.
- Se recomienda a servidores y funcionarios del Secap, que el equipo personal que usan fuera de la institución y que no pertenece a la misma, tenga un antivirus y antimalware instalado y debidamente actualizado.

7. Anexos

Ninguno.