POLÍTICA PARA LA RESTRICCIÓN EN LA INSTALACIÓN DE SOFTWARE

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 del Cambio

Versión	Fecha	Detalle de la modificación
1	03/03/2022	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.

La instalación de software en los equipos institucionales, es una actividad que debe estar debidamente regulada a través de políticas, con el fin de evitar que se instale software no requerido y que pueda poner en riesgo la seguridad de la información institucional.

3. Alcance

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

4. Propósito

Normar la instalación de software en los equipos institucionales del Secap, con el fin de restringir la instalación de aplicaciones o sistemas no requeridos por la institución y aquel que carece de las licencias de uso correspondientes.

5. Definiciones

- **Contraseña:** Código secreto compuesto por una cadena de caracteres que pueden ser especiales y alfanuméricos, que se introduce en un sistema, equipo informático o red para iniciarlo y acceder para operarlo.
- **Credenciales de acceso:** Son el nombre de usuario y contraseña gestionados que dan acceso a un sistema o equipo.
- **Dispositivos de almacenamiento extraíbles:** Son dispositivos que permiten el almacenamiento, transporte y transferencia rápida y directa de información; por

ejemplo: Memoria USB (flash memory/pendrive), discos ópticos (CD/DVD), discos duros externos (external HDD), tarjetas de memoria (SD Card, Mini SD, Micro SD).

- **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.
- **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 operativo:** Conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los diferentes periféricos o recursos de nuestra computadora, como son el teclado, el mouse, la impresora, la placa de red, entre otros.
- **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.
- **Unidad óptica:** También se les conoce como disco compacto (CD) o el disco digital versátil (DVD), son unidades de disco que utilizan una luz (óptico) láser como parte del proceso de lectura y escritura.
- **VPN:** Virtual Private Network o red privada virtual, es una conexión en línea caracterizada por ser segura y estar cifrada (codificada) que permite establecer comunicación desde un equipo remoto a una red empresarial o institucional.

6. Políticas

- La instalación y configuración de software o aplicaciones, es competencia única y exclusiva de la Dirección de Tecnologías de la Información y Comunicación.

- Ningún trabajador, servidor o funcionario de la institución está autorizado a instalar software o aplicaciones en los equipos que le han sido asignados, sin previa autorización de la DTIC.
- En caso de que se requiera instalar software o aplicaciones adicionales a las precargadas en los equipos institucionales, el servidor, funcionario o trabajador, deberá solicitar a la DTIC, a través del director de su área, la respectiva autorización, en la cual se justifique técnicamente la necesidad.
- El software o aplicación adicional que se requiera instalar, deberá tener la respectiva licencia de uso en caso de que sea de código pagado. Para casos de software o aplicaciones de código abierto o libre, éstas deberán ser debidamente evaluadas por personal de TIC a fin de prevenir que sean aplicaciones que incluyan virus o puedan afectar a la seguridad de la información.
- La DTIC, a través de la gestión de Administración de Servicios, Componentes de TI y Soporte Técnico a Usuarios, implementará los controles y restricciones de hardware y software que se requieran, a fin de evitar la instalación de software y aplicaciones no autorizadas.
- La DTIC podrá efectuar controles físicos aleatorios a los equipos institucionales para verificar la existencia de software o aplicaciones no autorizadas. En caso de encontrarse software o aplicaciones no autorizadas, el personal de la DTIC está autorizado a desinstalarlos del equipo en el cual se encontró, y notificar a la DTIC para que se tomen las acciones que correspondan.
- La DTIC podrá solicitar sanciones disciplinarias a los servidores, funcionarios y trabajadores que instalen software o aplicaciones sin la respectiva autorización.

7. Anexos

Ninguno.