POLÍTICAS DE EQUIPO INFORMÁTICO DE USUARIO DESATENDIDO

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
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	30/09/2021	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.

Para garantizar la seguridad de la información institucional, es importante tener claro cómo actuar en casos en los cuales los equipos informáticos de un usuario, están desatendidos; es decir, cuando el responsable del equipo no se encuentra en junto al mismo y éste está activo, por lo que cualquier persona podría usarlo y hacer cualquier actividad.

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, a través de políticas, un adecuado manejo de los equipos informáticos institucionales, con el fin de evitar que los mismos queden abiertos y sean considerados desatendidos.

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.
- **Equipo informático:** Conjunto de dispositivos electrónicos que permiten la ejecución de aplicaciones, sistemas o programas informáticos, también conocidos como computadoras.
- **Pantalla limpia:** Protección de los equipos de cómputo, tabletas, portátiles u otros dispositivos mediante un bloqueo de pantalla o desconexión cuando no está en uso.
- **Puesto de trabajo:** Área y mobiliarios dispuesto por la institución para que un servidor, funcionario o trabajador puedan llevar a cabo sus actividades.
- **Servidor / Funcionario / Trabajador:** 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.
- **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.
- **Usuario desatendido:** Equipo informático que se encuentra activo, con libre acceso y sin protección de ningún tipo, que puede ser usado por cualquier persona en cualquier momento.

6. Políticas

- Todo servidor, funcionario o trabajador dispondrá, en su área de trabajo, de un lugar debidamente adecuado para la ubicación de los equipos informáticos que se le han asignado, mismos que no deben estar expuestos al acceso de personas externas.
- Para servidores, funcionarios o trabajadores encargados de la atención al público, los equipos informáticos deben estar ubicados de forma segura, sin que puedan ser vistos por personas externas y sin la posibilidad de que puedan acceder a los mismos por dichas personas.

- Es responsabilidad del servidor, funcionario o trabajador el cuidado y buen uso del equipo informático asignado.
- Todo equipo informático tendrá credenciales de acceso (usuario y contraseña), tanto para iniciar sesión en el sistema operativo, así como para las diferentes aplicaciones o sistemas informáticos institucionales.
- El servidor, funcionario o trabajador que deba ausentarse de su lugar de trabajo, deberá bloquear, suspender o apagar su equipo informático, a fin de evitar accesos no deseados.
- Todo servidor, funcionario o trabajador que encontrare o visibilizare equipos informáticos sin la cercanía de su custodio o responsable, y esté desatendido, deberá bloquearlo inmediatamente y notificar del particular al responsable de dicho equipo y su inmediato superior.
- Los dispositivos móviles asignados a un servidor, funcionario o trabajador, estos deberán estar configurados con la opción de cierre automático o bloqueo por inactividad, y de desbloqueo con contraseña, patrón o huella digital.

7. Anexos

Ninguno.