



INSTITUTO TECNOLÓGICO  
SUPERIOR DE CAJEME

DEPARTAMENTO DE  
SISTEMAS

MANUAL DE POLÍTICAS Y  
LINEAMIENTOS DE TECNOLOGÍAS  
DE LA INFORMACIÓN

---

SEPTIEMBRE 2023.

## ÍNDICE

OBJETIVO GENERAL.....	3
OBJETIVOS ESPECÍFICOS .....	3
ALCANCE .....	3
CONSIDERACIONES GENERALES.....	3
CONTRASEÑAS .....	4
CORREO ELECTRÓNICO E INTERNET .....	4
USO DE SOFTWARE .....	5
POLÍTICAS PARA EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.....	5
GENERALES.....	5
EQUIPO DE CÓMPUTO.....	5
ÁREA DE SERVIDORES .....	6
PROPIEDAD DE LA INFORMACIÓN.....	6
USOS INADECUADOS.....	7
EXCEPCIONES.....	7
POLÍTICA DE CONTRASEÑAS.....	8
PROHIBICIONES DE LAS CONTRASEÑAS .....	8
POLÍTICAS DE USO DE INTERNET Y CORREO ELECTRÓNICO .....	8
CORREO ELECTRÓNICO .....	9
INTERNET.....	9
SEGURIDAD .....	9
POLITICAS DE USO E INSTALACION DE SOFTWARE.....	10
POLÍTICAS Y REGLAMENTO DE CENTROS DE COMPUTO .....	10
POLITICAS USO DE INTERNET EN AULAS ACTIVAS Y CENTRO DE COMPUTO .....	10
REGLAMENTOS DE LOS CENTROS DE COMPUTO .....	11
VIGENCIA DE LAS POLÍTICAS.....	12

## **OBJETIVO GENERAL**

El objetivo general de este manual es establecer las políticas de seguridad de Tecnologías de Información y Comunicaciones, para el uso correcto de las mismas dentro del Instituto Tecnológico Superior de Cajeme, las cuales se relacionan a continuación:

- Políticas para el uso adecuado de las Tecnologías de la Información y Comunicaciones.
- Políticas del uso de contraseñas.
- Políticas del uso de internet y correo electrónico.
- Políticas del uso de software.

## **OBJETIVOS ESPECÍFICOS**

- Dar a conocer las políticas del uso de las TIC'S.
- Dar a conocer las políticas del uso de contraseñas.
- Dar a conocer las políticas del uso de internet y correo electrónico.
- Dar a conocer las políticas del uso de software.

## **ALCANCE**

Las políticas son aplicables para todos los usuarios de las diferentes áreas administrativas que utilicen equipo de cómputo, Los usuarios tienen la obligación de seguir al pie de la letra las presentes políticas emitidas por Centro de Cómputo y aprobadas por Dirección General.

El Centro de Cómputo es el área encargada de administrar estas políticas. Estas políticas aplican al equipo de cómputo resguardado y registrado como activo fijo en el ITESCA.

## **CONSIDERACIONES GENERALES**

Las políticas definidas en este punto están relacionadas con los equipos de cómputo que son asignados a los usuarios de las diferentes áreas administrativas, aspectos relacionados con la propiedad de la información que es creada y manipulada por los usuarios del ITESCA y la utilización inadecuada de los recursos informáticos que el ITESCA pone a disposición de sus empleados para que desarrollen sus actividades. Constituye la base de las políticas que debe cumplir todo el personal.

## **CONTRASEÑAS**

El cumplimiento de las políticas de contraseñas por parte de los usuarios del ITESCA, es de suma importancia ya que estas constituyen la primera línea de defensa para garantizar que la información solo sea accedida por el personal autorizado. Tanto para equipos, sistemas y datos que utilizan mecanismos de contraseñas para controlar el acceso a ellos, un ejemplo de ello es la contraseña que se utiliza en el momento en que se inicia el equipo, para ingresar a las diferentes redes que se tienen en el ITESCA, como tal los usuarios son los responsables de las contraseñas que se utilizan en sus equipos, centro de cómputo es responsable de las diferentes contraseñas que se utilizan para acceso a la red así como a los diversos sistemas que se operan en ITESCA.

## **CORREO ELECTRÓNICO E INTERNET**

Los accesos a internet y correo electrónico son servicios que actualmente se utilizan en las diferentes áreas del ITESCA tanto para docentes como para personal administrativo y dirección general con los siguientes beneficios:

- Se tiene una instalación de red funcional que es proporcionada por un proveedor, con ella se tiene acceso a internet.
- Se ofrece a los usuarios servicio de correo electrónico que es proveído por Microsoft con un dominio @cajeme.tecnm.mx y Google con dominio @itesca.edu.mx, con ello se interactúa de forma ágil y eficiente de manera interna, así también con las diferentes dependencias gubernamentales relacionadas con el ITESCA.
- Los correos institucionales proporcionados a las y los trabajadores de ITESCA, deberán ser usados únicamente para uso institucional y en relación a sus labores que desempeñen en su puesto y evitar ser usado para asuntos de índole personal ya que los derechos de esa información pasarán a pertenecer a ITESCA, cuando las o los trabajadores causen baja de la institución, las cuentas inmediatamente se suspenden y la información almacenada en dichas cuentas será para uso exclusivo de la institución. Por tal motivo el ex trabajador o ex trabajadora perderá todos los derechos de acceso a la información, aunque sea de índole personal, y no se debe considerar como datos personales, ya que el correo es exclusivamente para uso laboral.

El correo electrónico e Internet se ha convertido en medios de comunicación indispensables para el trabajo diario en el ITESCA es por ello que se deben de cumplir con las políticas relacionadas con dichos servicios así, se evitan interrupciones que podrían afectar en las diferentes tareas que se realizan dentro del ITESCA.

## **USO DE SOFTWARE**

Los programas o software están protegidos por las leyes de derechos de autor, algunas veces se ignora el hecho de que el software tiene un valor económico, sin embargo, el software es un elemento crítico en varios aspectos de funcionamiento dentro del ITESCA por lo tanto debe administrarse y tener políticas de uso.

Las políticas del uso de software dentro del ITESCA se crean para que sirvan como marco regulatorio en cuanto a la instalación y el uso del mismo en el equipo de cómputo que es propiedad del ITESCA.

## **POLÍTICAS PARA EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**

### **GENERALES**

- Bajo ninguna circunstancia los usuarios tienen permitido hacer mal uso del software instalado en los diferentes equipos del ITESCA, así también realizar actividades prohibidas por las normas jurídicas nacionales o internacionales.
- El Centro de Cómputo es el área responsable de realizar actividades de soporte técnico y realizar cambios a la configuración del mismo. En caso del mantenimiento que deseen ejecutar terceras personas o ajenas al centro de cómputo deberán realizarse con previa autorización por el responsable del mismo. En el caso de los equipos que son arrendados al ITESCA la empresa arrendadora es la responsable de hacer las labores de mantenimiento y de cambio de hardware o en su caso autorizar al responsable del centro de cómputo efectuar dichas labores.

### **EQUIPO DE CÓMPUTO**

- El equipo de cómputo propiedad del ITESCA, deberá ser utilizado únicamente para actividades relacionadas con los objetivos y metas del Instituto.
- Para el correcto funcionamiento del equipo de cómputo deberán realizarse como mínimo dos mantenimientos preventivos al año. El plan de mantenimiento será realizado por el responsable del centro de cómputo en los meses de Julio y diciembre del año en curso.
- Centro de Cómputo deberá implementar acciones necesarias para el correcto funcionamiento del equipo de cómputo del ITESCA.
- Para la adquisición de material o refacciones para el equipo de cómputo, se deberá hacer mediante solicitud de recursos materiales F01PDA20.10 formato que se encuentra dentro del Sistema de gestión de calidad (SGC) la cual deberá ser autorizada por la Subdirección de Planeación y Recursos Materiales.
- Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa a un equipo de cómputo del ITESCA, deberá ser notificado al jefe

departamento TIC, subdirección de planeación, jefe de seguridad, vigilancia y al encargado de centro de cómputo.

- Solo el personal autorizado por el responsable del centro de cómputo y personal de mantenimiento preventivo podrá abrir los gabinetes de las computadoras personales o cualquier otro equipo del ITESCA. Para los equipos de cómputo arrendados, la empresa arrendadora es la única autorizada para abrir los gabinetes de los equipos o en su caso dar mantenimiento y soporte.
- Todos los equipos que sean propiedad del ITESCA, deberán contar con un software antivirus actualizado con el objetivo de mantenerlos seguros de programas maliciosos como: virus informáticos, gusano informático, virus troyano, spyware, malware, adware, ransomware.
- Para conectar un equipo a la red institucional, el responsable del centro de cómputo o encargado del área de mantenimiento deberá revisar el equipo de cómputo, así mismo si requiere ser formateado, se realice para poder ingresarlo a la red institucional, sin propagar ningún virus informático, además se hace una evaluación del porque se desea acceder a la red institucional y si es viable.
- Todo equipo de cómputo propiedad del ITESCA deberá ser registrado en la base de datos para tener un control de acceso a la red.

## **ÁREA DE SERVIDORES**

El área de servidores es la zona donde se alojan los equipos de comunicación necesarios para realizar actividades informáticas del Instituto.

- Solo el personal autorizado tiene acceso a dicha área.
- Solo el personal autorizado por centro de cómputo puede abrir el gabinete de los servidores.
- Se puede acceder a los servidores ya sea vía remota utilizando software especializado y solo el personal autorizado por centro de cómputo tendrá acceso, cualquier conexión remota no autorizada será considerada como violación a las políticas de seguridad.

## **PROPIEDAD DE LA INFORMACIÓN**

- Los usuarios de cualquier equipo de cómputo del ITESCA deben estar conscientes que toda la información que crean y/o manipulan en los diferentes sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son propiedad y responsabilidad del ITESCA.
- Los derechos patrimoniales de un programa de cómputo, hojas de cálculo, archivos de Word, Power Point, etc. y su documentación, creada por uno o varios usuarios en el ejercicio de sus actividades laborales corresponden al ITESCA.

- Los respaldos que contengan información del ITESCA y que fueron realizados o solicitados por el usuario del equipo de cómputo, se tendrán bajo resguardo por el área de recursos materiales.

## **USOS INADECUADOS**

### ***Las siguientes actividades están prohibidas:***

1. Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de la Información.
2. Introducir software malicioso en la red o en los servidores (virus, gusanos, troyanos, etc.)
3. Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o los servicios.
4. Monitorear puertos o realizar análisis del tráfico de la red con el fin de evaluar las vulnerabilidades de seguridad. El responsable del centro de cómputo puede realizar estas actividades para realizar mejoras a la red y solventar las vulnerabilidades.
5. Ejecutar herramientas de monitoreo de la red de manera no autorizada.
6. Burlar las contraseñas de los diferentes usuarios para poder acceder a los equipos, el responsable del centro de cómputo puede realizar esta actividad siempre y cuando el usuario de previa autorización.
7. Instalar cualquier tipo de software en los equipos de cómputo del ITESCA sin la previa autorización del responsable del centro de cómputo.
8. Modificar la configuración de los equipos de cómputo con el fin de dañar el sistema operativo o aplicaciones que son útiles para las diferentes tareas de los usuarios.
9. Desconectar periféricos de los equipos de cómputo (teclado, mouse, cable de red, cables de video VGA o HDMI, cables de corriente etc.), sin autorización del encargado de centro de cómputo; Si se le autoriza, al finalizar deberá dejarlo como estaba al recibirlo.
10. Hacer uso de aplicaciones de transmisión en vivo para reproducir música que no estén autorizadas por el responsable del centro de cómputo.
11. Realizar descargas de archivos no permitidos (películas, música, etc.) desde internet.

## **EXCEPCIONES**

Para propósitos de mantenimiento a la red, el responsable del centro de cómputo está exento de seguir algunas restricciones anteriores, debido a las responsabilidades de su cargo o por eventos programados.

Estas excepciones deben ser autorizadas por la Subdirección de Servicios Administrativos.

## **POLÍTICA DE CONTRASEÑAS**

1. Los usuarios pueden utilizar contraseñas en sus equipos, el responsable del centro de cómputo tiene la autorización de resetear la contraseña si es que el usuario la ha olvidado.
2. Por seguridad las contraseñas deben ser actualizadas cada cierto tiempo por el usuario.
3. Las contraseñas de correo electrónico son generadas por el administrador de correo, al generar la cuenta del usuario, se le pide que actualice su contraseña para poder acceder a ella, las contraseñas pueden ser restablecidas desde el administrador de correo por el responsable del centro de cómputo.
4. Las contraseñas deben ser resguardadas por los usuarios hasta el término de la relación laboral, todas las contraseñas que el usuario maneje, deben ser proporcionadas al nuevo personal o en su defecto al responsable del centro de cómputo.

## **PROHIBICIONES DE LAS CONTRASEÑAS**

1. Revelar la contraseña a personal no autorizado o permitir el uso a terceros para actividades ajenas a la misión del ITESCA. La prohibición incluye a cualquier persona que no tenga relación con las actividades que se realizan en el Instituto.
2. Anotar la contraseña en un Post-it o en cualquier otro medio físico y que esté a la vista de todos en el lugar de trabajo. Se recomienda que la contraseña se aprenda de memoria y no anotar en ningún medio físico como libretas, se puede almacenar en algún software especializado para el resguardo de las mismas.

## **POLÍTICAS DE USO DE INTERNET Y CORREO ELECTRÓNICO**

Los servicios de Acceso a Internet y Correo Electrónico son administrados por el responsable del centro de cómputo quien realiza los reportes de falla en el servicio de internet, así como también apoyar a los usuarios en los temas relacionados a su correo electrónico, sin embargo, el proveedor del enlace a internet es el responsable de garantizar la disponibilidad del enlace, así como de los anchos de banda contratados.

El responsable del centro de cómputo se encarga de monitorear los diferentes puntos de acceso a internet, en dado caso de alguna falla deberá de realizar las actividades correctivas pertinentes para restablecer la conexión a los diferentes equipos conectados.

## **CORREO ELECTRÓNICO**

1. La comunicación se realiza por correo electrónico y esta solo será a través de cuentas institucionales asignadas.
2. El Correo Electrónico es para envío de correspondencia privada entre emisor y el destinatario, por lo tanto, la información no deberá ser distribuida vía internet considerada como confidencial hacia personas o instituciones externas a menos que dirección general, subdirecciones o jefes de departamento lo autorice.
3. El usuario es responsable del contenido de los mensajes enviados, esto incluye entre otros: contenido de material ofensivo y obsceno, cualquier violación a la propiedad intelectual, copyright o cualquier información legal.
4. Se prohíbe enviar SPAM a los diferentes usuarios que laboran en el ITESCA.

## **INTERNET**

1. Los usuarios son responsables del uso que le dan al servicio de internet.
2. Los equipos que deseen conectarse a la red, deberán ser registrados en una base de datos para tener acceso.
3. Los usuarios que requieran conexión a la red, deberán solicitar el acceso al responsable del centro de cómputo.
4. Acceder, ver o descargar desde sitios de internet imágenes, vídeos o cualquier otro material que pueda ser considerado como obsceno, abusivo u ofensivo, con lenguaje amenazante y otra forma de lenguaje objetable dirigido a un individuo o grupo.

## **SEGURIDAD**

1. El centro de cómputo es responsable de proporcionar el servicio otorgando los accesos a los diferentes puntos de acceso.
2. Las cuentas de correo electrónico son personales y confidenciales y se rigen por las políticas de contraseñas definidas en el presente documento.
3. El usuario notificará inmediatamente al responsable del centro de cómputo cualquier uso no autorizado de su cuenta o cualquier intrusión de seguridad que pueda llegar a suscitarse.
4. El usuario tiene la obligación de usar los servicios con fines institucionales.

5. Se prohíbe el acceso, descarga o transmisión de material cuyo origen sea considerado como inseguro o de aquel que se desconozca su confiabilidad.
6. Cualquier archivo o programa descargado de internet deberá ser analizado con un antivirus.
7. No se permite utilizar el correo electrónico institucional para realizar suscripciones en páginas de transmisión en línea o alguna otra página que pueda saturar el correo electrónico institucional.

## **POLÍTICAS DE USO E INSTALACIÓN DE SOFTWARE**

El responsable del centro de cómputo en conjunto con el jefe departamento de TIC, son los encargados de llevar a cabo el inventario y el resguardo de las diferentes licencias que se tienen en el ITESCA, entre sus responsabilidades están:

- Mantener bajo resguardo las licencias de uso de software.
- Tener un inventario de las licencias.
- Difundir a los usuarios las Políticas de Uso de Software con el fin de que conozcan la normatividad en este rubro.
- Realizar un análisis de las necesidades y requerimientos de Software, con la finalidad de presentarlo a Dirección General y a la Subdirección de Servicios Administrativos quienes autorizan la adquisición.
- El personal docente, deberá de solicitar vía correo electrónico, la instalación del software necesario, especificando los siguientes requerimientos:
  - Nombre del Software
  - Versión del Software
  - Liga de acceso en caso de ser necesario descargarlo vía internet
  - Cantidad de equipos que se requiere instalar
  - Aulas donde se requiere la instalación del Software
  - Fecha en la que se requiere que sea instalado y tomar en cuenta una semana previa a la fecha de la instalación para hacer la solicitud, para que la instalación pueda ser programada y estar a tiempo.

## **POLÍTICAS Y REGLAMENTO DE CENTRO DE COMPUTO**

### **POLITICAS USO DE INTERNET EN AULAS ACTIVAS Y CENTROS DE COMPUTO.**

- Internet en horario de clases, las y los alumnos, deberán de hacer uso adecuado en las navegaciones y acatar las indicaciones que le brinde el profesor(a).

- El Instituto Tecnológico Superior de Cajeme, en caso de llevar a cabo un evento académico y que se requiera de los recursos informáticos como el internet, deberá de notificar con anticipación a la comunidad de ITESCA, que los servicios serán interrumpidos en determinado tiempo.

## **REGLAMENTOS DE LOS CENTROS DE COMPUTO**

- Vacunar cualquier dispositivo externo de almacenamiento (USB o Discos portables).
- No introducir alimentos ni bebidas.
- No fumar en el interior de los laboratorios de cómputos.
- Trabajar una sola persona por computadora, sin excepción alguna.
- No se permite instalar ningún tipo de software a la PC.
- Estrictamente prohibido todo tipo de CHAT y consulta de páginas de contenido inapropiado (Redes Sociales, pornografía, etc)
- No cambiar la configuración del equipo en protector de pantalla, colores de videos, fondos de pantalla, contraseñas locales.
- Mantener el área de trabajo limpia y ordenada.
- Todo aquel alumno que, al terminar de utilizar el equipo, deberá de acomodar su silla en su lugar
- Se deberá de trabajar en silencio y orden
- Si la o el alumno deseara escuchar cualquier tipo de audio, deberá de contar con audífonos.
- Los trabajos escolares tendrán prioridad, ante todo.
- En caso de un problema técnico, se le deberá avisar al encargado en turno, de no ser así, se le responsabilizará el usuario(a) de algún daño en el equipo.
- Los usuarios no desconectaran los periféricos de los equipos de cómputo (teclado, mouse, cable de red, cables de video VGA o HDMI, cables de corriente etc.)

- los equipos de cómputo, sin autorización del encargado del área.
- Todo aquel usuario(a) que desee utilizar un equipo de los laboratorios de cómputo y/o aulas activas, deberá de poner su celular en modo vibración.
- Toda persona que no acate este reglamento será sancionada. La sanción dependerá de la infracción realizada.

## **VIGENCIA DE LAS POLÍTICAS**

Estas políticas tendrán vigencia a partir de su aprobación por Dirección General y serán revisadas por el responsable del centro de cómputo, jefe departamento de TIC, Subdirección de Planeación, Servicios Administrativos y por el comité de TIC conforme surjan cambios en la infraestructura o evolución tecnológica.

**FECHA DE CREACIÓN:** 30 DE MARZO 2022

**ULTIMA MODIFICACIÓN:** 18 DE SEPTIEMBRE DE 2023

**VERSIÓN:** 1.4