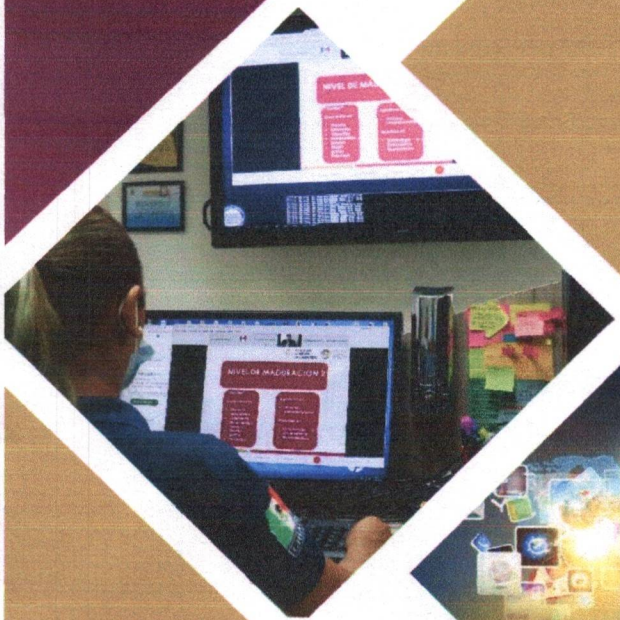
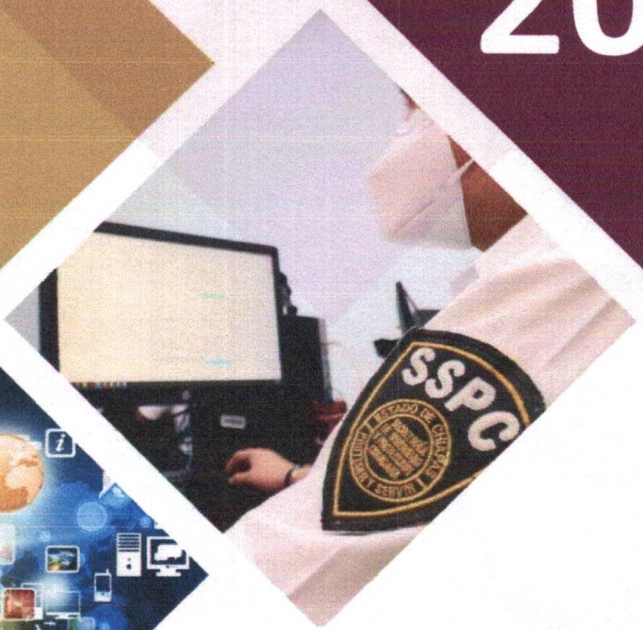
CHIAPAS
GOBIERNO DEL ESTADO

SECRETARÍA
DE SEGURIDAD Y
PROTECCIÓN CIUDADANA
GOBIERNO DE CHIAPAS

2023





MANUAL DE POLÍTICAS PARA EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA.

UNIDAD DE TECNOLOGÍAS Y GESTIÓN DE LA INFORMACIÓN.

CHIAPAS de Corazón

INDICE

ANTECEDENTES

En términos del artículo 43 de la Ley Orgánica de la Administración Pública del Estado de Chiapas, concatenado al consecutivo 2 párrafo segundo, de la Ley que Establece las Bases de Operación de la Secretaría de Seguridad y Protección Ciudadana del Estado de Chiapas, en relación al artículo 1, del Reglamento de Ética y Disciplina de la Secretaría de Seguridad y Protección Ciudadana, los integrantes de la Secretaría de Seguridad y Protección Ciudadana, en su calidad de servidores públicos, deberán su actuación con apego a la ética y disciplina, así como, obediencia, justicia y un alto sentido del honor.

En ese tenor, las y los servidores públicos de la Secretaría de Seguridad y Protección Ciudadana, deberán ser diligentes en el uso de los sistemas de información, en el manejo de tecnologías de la información y bienes informáticos observando en todo momento el presente Manual de Políticas para el Uso de Tecnologías de la Información de la Secretaría de Seguridad y Protección Ciudadana.

La aplicación de las tecnologías de la información en las actividades propias de las instituciones gubernamentales se encuentra regulada por la Normatividad para la Gestión y Desarrollo de Tecnologías de Información y Telecomunicaciones, para aplicación y seguimiento en beneficio de los esfuerzos por aprovechar el potencial que ofrecen las tecnologías de información, así mismo, validan el proceso, desarrollo o adquisición de bienes informáticos; con ello, se visualiza los estándares de uso de tecnologías y resguardo de la confidencialidad de la información. De igual manera, es de observancia general y obligatoria.

En ese contexto, la Secretaría de Seguridad y Protección Ciudadana bajo el amparo del artículo 15 párrafo segundo de la Ley Orgánica de la Administración Pública del Estado de Chiapas, emite el presente Manual de Políticas de Tecnologías de la Información de la Secretaría de Seguridad y Protección Ciudadana, es una herramienta que garantiza la gestión, uso, administración, mantenimiento y funcionamiento de los bienes informáticos, de la Secretaría de Seguridad y Protección Ciudadana, para contribuir con la eficiencia y optimizar los sistemas internos, asegurando la seguridad de la información.

ASPECTOS GENERALES

Objetivo

Trazar lineamientos del uso de las tecnologías de la información, a fin de facilitar la optimización de los sistemas internos, calidad de gestión, conservación y seguridad de la infraestructura tecnológica, confidencialidad e integridad de la información Institucional.

Marco Legal

- Ley Orgánica de la Administración Pública del Estado de Chiapas.
- Ley que Establece las Bases de Operación de la Secretaría de Seguridad y Protección Ciudadana del Estado de Chiapas.
- Reglamento de la Ley que Establece las Bases de Operación de la Secretaría de Seguridad y Protección Ciudadana del Estado de Chiapas.
- Reglamento del Comisión de Honor y Justicia de la Secretaría de Seguridad y Protección Ciudadana.
- Reglamento de Ética y Disciplina de la Secretaría de Seguridad y Protección Ciudadana.
- Normatividad para la Gestión y Desarrollo de Tecnologías de Información y Telecomunicaciones vigente en el Estado de Chiapas.

CONSIDERACIONES GENERALES

Se consideran regidos por este Manual, todas las tecnologías de la información que se utilicen dentro de la Secretaría de Seguridad y Protección Ciudadana, aún aquellos que no sean propiedad de la misma, pero que puedan afectar el funcionamiento de los servicios y sistemas.

I. De la Unidad de Tecnologías y Gestión de la Información:

a. Es la instancia inmediata encargada de la vigilancia, supervisión y cumplimiento de los presentes lineamientos.
b. Deberá difundir estos lineamientos entre los usuarios.
c. Diseñar los procedimientos que aseguren el cumplimiento del Manual de Políticas de Tecnologías de la Información de la Secretaría de Seguridad y Protección Ciudadana.
d. El personal adscrito a la Unidad de Tecnologías y Gestión de la Información, está autorizado para monitorear los sistemas de información de la Secretaría de Seguridad y Protección Ciudadana, para salvaguardar la integridad, disponibilidad, seguridad y desempeño correcto de los mismos y ejecutar las acciones pertinentes como: negación, restricción de acceso de usuarios o sistemas, aislamiento y desconexión de equipos o servicios.

II. De los Usuarios:

a. Están obligados a conocer los presentes lineamientos.
b. El personal operativo y administrativo deberán acatar en todo momento el Decreto de Austeridad, Disciplina y Racionalidad del Gasto, priorizando el uso de sistemas de información para la gestión de documentos de manera digital.
c. El usuario será responsable de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este Manual.

III. Para los efectos de este Manual, se entenderá por:

1. **Tecnología de la Información (TI)**. - El conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, etc.). El elemento más representativo de las nuevas tecnologías es sin duda el ordenador y más específicamente, Internet.

2. **Software**. - Término informático que hace referencia a un programa o conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

3. **Hardware**. - Parte física de un ordenador o sistema informático. Está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos, cables eléctricos, tarjetas madre, memorias, discos duros, dispositivos periféricos y cualquier otro material en estado físico que sea necesario para hacer que el equipo funcione.

4. **Sistema operativo**. - Son los programas encargados de administrar y gestionar de manera eficiente todos los recursos de un ordenador y otros dispositivos; gestiona el funcionamiento del hardware del equipo, además de poner en marcha las herramientas y funciones que hacen que un ordenador pueda comunicarse e interactuar con quien lo está utilizando, y viceversa.

5. **Aplicación (también llamada app)**. - Programa informático creado para llevar a cabo o facilitar una tarea en un dispositivo informático. Cabe destacar que, aunque todas las aplicaciones son programas, no todos los programas son aplicaciones. Existe multitud de software en el mercado, pero sólo se denomina así a aquel que ha sido creado con un fin determinado, para realizar tareas concretas. No se consideraría una aplicación, por ejemplo, un sistema operativo, pues su propósito es general.

6. **Sistema de información**. - Conjunto de datos que interactúan entre sí, con un fin común, ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.

7. **Base de datos**. - Conjunto de información que se relaciona entre sí, que está almacenada y organizada de forma sistemática para facilitar su preservación, búsqueda y uso.

8. **Bien informático. -** Cualquier elemento que forma parte del sistema técnico del ordenador, comprendidos tanto la unidad central de procesamiento como el resto del soporte físico del elemento informático. Son también bienes informáticos los datos, procedimientos e instrucciones que contribuyen al tratamiento automatizado de la información.

9. **CPU**. - Sigla en inglés de Central Processing Unit, traducido al español como la **Unidad Central de Procesamiento de un Dispositivo Electrónico**, como una computadora, un teléfono móvil, una tablet, una consola de videojuegos, etc.

10. **Periféricos**. - Son aquellos dispositivos auxiliares independientes de la unidad central de procesamiento o CPU de un ordenador, un conjunto de dispositivos electrónicos físicos que, sin pertenecer al núcleo fundamental de la computadora, formado por la CPU y la memoria central, permitan realizar operaciones de entrada/salida (E/S) complementarias al proceso de datos que realiza la CPU.

11. **Seguridad de la información**. - Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

12. **Confidencialidad de la información**. - Tratamiento que se le da a los datos, para evitar la divulgación y/o acceso no autorizado de la información.

13. **Integridad de la información**. - Implica mantener la consistencia, precisión y confiabilidad de los datos durante todo su ciclo de vida. Estas medidas incluyen permisos de archivos y controles de acceso de usuarios.

14. **Disponibilidad de la información**. - Garantizar el acceso a la información, mediante el cumplimiento de reglas de seguridad establecidas.

15. **Malware.** - Es un acrónimo del inglés de malicious software, traducido al español como **código malicioso**. Los malwares son programas diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información.

16. **Virus**. - Es un software dañino que, una vez instalado en una computadora (ordenador), puede destruir los datos almacenados.

17. **Spyware.** - Estos programas están diseñados para monitorear la navegación web de los usuarios. El spyware no se propaga como los virus, normalmente se instala aprovechando las vulnerabilidades de seguridad, también, se pueden ocultar y empaquetar con software no relacionado instalado por el usuario.

18. **Rootkit.** - Este malware permite al hacker instalar una serie de herramientas para acceder de forma remota al equipo, normalmente oculto en el sistema operativo, no es detectado por el software antivirus y otras herramientas de seguridad. El rootkit puede recopilar contraseñas, robar información de tarjetas y cuentas bancarias online y desactivar software de seguridad.

19. **Troyanos. –** Es un malware utilizado para robar información de un equipo de cómputo.
Al ser activados o abiertos, permite el acceso no autorizado a datos en el computador o sistema informático infectado.

20. **Gusanos**. - Se alojan en un sistema creando copias infinitas de sí mismos, con la finalidad de colapsar la red o el dispositivo bloqueando cualquier trabajo adicional.

21. **Adware**. - Es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador web.

22. **Dialer.** - Es un programa que usa el módem del ordenador para realizar llamadas de tarificación adicional, mediante una conexión de marcación sobre internet, obteniendo dinero de las llamadas.
La conexión se realiza con la marcación a un determinado número telefónico y conectándose a números de teléfonos internacionales o premium locales. Los dialers son capaces de realizar conexiones no autorizadas y sobrepasar el proveedor de servicios de internet local, tras ejecutar estas actividades, las víctimas pierden dinero con un incremento de los recibos de las facturas telefónicas.

23. **Keyloggers.** - Realizan un seguimiento y registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario.

24. **PUP.**- Potentially Unwanted Program (programa no deseado), pueden afectar el rendimiento del ordenador, así como violar la privacidad del usuario. Tomemos como ejemplo el adware, un tipo común de PUP, puede añadir complementos en el navegador del usuario y monitorear sus actividades en internet, en muchas ocasiones, esta información se vende a anunciantes, quienes la utilizarán para mostrar publicidad intrusiva en páginas web.

25. **Proxy.** - Es una tecnología que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (internet), es comúnmente utilizado para acceder a servicios que tienen bloqueado su contenido.

26. **Vulnerabilidad.** - Es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un "agujero" que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño

27. **Filtro web.** - Comúnmente conocido como "software de control del contenido", es un software diseñado para restringir los sitios web que un usuario puede visitar en su equipo.

28. **Control de aplicaciones**. - Se utiliza para implementar una política de seguridad corporativa que regule el uso de aplicaciones en los equipos de los usuarios. El componente también ayuda a reducir el riesgo de que los equipos se infecten.

29. **Monitoreo de red.** - Proporciona la información que los administradores necesitan para determinar si una red está funcionando de manera óptima, mediante el monitoreo y análisis del tráfico de la red en tiempo real, inventariado de activos y gestión de software y licencia.

30. **Violación de seguridad.** - Cualquier acción que provoque la pérdida o alteración de algún dato, así como una comunicación a terceros no autorizada.

31. **Ataque o incidente de seguridad.** - Es un evento o serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer la operatividad institucional; provocando una pérdida o uso indebido de información, interrupción parcial o total de los sistemas, siendo los más comunes, la infección por malware, phishing, etc.

32. **Política de control de acceso a la información**. - Serie de reglas y configuraciones aplicados a los usuarios utilizados por los empleados para tener acceso únicamente a la información mínima con la que puedan desarrollar su actividad laboral.

33. **Red de datos.** - Es una red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el

transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

34. **Correo electrónico. -** (también conocido como **e-mail**, un término inglés derivado de electronic mail) es un servicio que permite el intercambio de mensajes en los que se pueden incluir todo tipo de información.

35. **Internet. -** Es una red de computadoras que se encuentran interconectadas a nivel mundial para compartir información.

36. **Streaming. -** Transmisión de contenido multimedia como películas, series o videos.

37. **Usuarios. -** Son individuos que utilizan habitualmente programas, aplicaciones, sistemas, computadoras, tabletas electrónicas o teléfonos inteligentes.

38. **Perfil de usuario**. - Se emplea en el ámbito de la informática. Así se denomina a un entorno personalizado para un individuo que se desarrolla de acuerdo a sus preferencias de configuración.

39. **Credenciales de acceso. –** Son los nombres de usuario y contraseñas gestionados que dan acceso a diversas aplicaciones.

POLÍTICAS Y NORMAS

De las Cuentas, su Uso y Privacidad

Las credenciales de acceso a la red de datos interna, correo electrónico, sistemas de información y otros servicios informáticos propiedad de la Secretaría de Seguridad y Protección Ciudadana, son para empleo institucional exclusivamente y queda bajo la más estricta responsabilidad del usuario su extravío o mal uso.

El usuario de equipo informático a quien personal de la Unidad de Tecnologías y Gestión de la Información, le designe usuario y contraseña de cuenta, quedará bajo su más estricta responsabilidad el uso y fin de las mismas.

En caso de que el equipo informático a ~~su~~ resguardo del usuario, requiera reparación, deberá proporcionar usuario y contraseña al personal de la Unidad de Tecnologías y Gestión de la Información; dejando a salvo la opción de solicitar la asignación de nuevo usuario y contraseña.

Una vez terminada la relación laboral del usuario con la Secretaría de Seguridad y Protección Ciudadana, al ser notificada a la Unidad de Tecnologías y Gestión de la Información, ésta procederá a inhabilitar las cuentas de usuario y transferir toda la información que haya creado durante el periodo laboral al personal designado.

Las cuentas de usuarios serán desactivadas de manera automática, cuando el personal propietario de éstas se encuentre de vacaciones, incapacitados o con licencia y serán reactivadas automáticamente de acuerdo a las actualizaciones que el Área de Recursos Humanos haga en el Sistema "Kronos".

Se usará autenticación de doble factor, por lo que se asociará el número de teléfono celular de cada usuario a su perfil, mediante el cual, recibirá los códigos de verificación que le permitirán el acceso a los sistemas de información, así mismo, podrá recuperar su cuenta de usuario y contraseña de manera más rápida.

Es obligación de cada usuario, mantener actualizada la información personal asociada a su cuenta (número de celular, correo electrónico).

En ningún caso es permitido el intercambio de cuentas de acceso entre usuario.

De los Bienes Informáticos

El uso de los bienes informáticos (equipos, software, aplicaciones, sistemas de información, bases de datos, periféricos, documentos e información) propiedad de la Secretaría de Seguridad y Protección Ciudadana, serán asignados al personal adscrito a la misma mediante el resguardo correspondiente y serán utilizados únicamente para llevar a cabo las actividades laborales que le fueron asignadas en el área donde se encuentre adscrito.

El mal uso o el daño intencional a los recursos tecnológicos institucionales, se dará vista a la Unidad de Asuntos Internos para que sea quien determine o deslinde responsabilidades de acuerdo a la normatividad aplicable.

Los recursos de impresión, deberán ser utilizados con fines de apoyo en las labores diarias y propias de la función que desempeña, por lo que, no es permitida la impresión de trabajos personales. Así mismo no está permitida la impresión de materiales que infrinjan de alguna forma los derechos de autor, tampoco está permitida la impresión de grandes volúmenes que afecten el funcionamiento de los equipos de impresión y que utilicen en exceso materiales y consumibles.

No deberá usar los bienes informáticos para acceso, descarga, transmisión, distribución o almacenamiento de material obsceno, ilegal, nocivo o que infrinja los derechos de autor o que no tenga autorización para su uso y/o distribución.

No está permitido el uso de los bienes informáticos para generar ganancias económicas personales o desarrollar actividades o labores de terceros.

Los equipos de cómputo, software y aplicaciones instaladas en ellos, deberán ser usados únicamente por el o los usuarios designados para dicho fin.

El personal adscrito a la Secretaría, que requiera hacer uso de los equipos, software, servicios y periféricos de esta institución para fines de estudios e investigaciones

académicas, deberá solicitar autorización al titular de la Unidad de Tecnologías y Gestión de la Información.

La Unidad de Tecnologías y Gestión de la Información, a través de su titular, es el facultado para emitir la autorización a que refiere el párrafo anterior, siempre que no interfiera en las actividades asignadas al puesto, cargo o comisión tanto operativas como administrativas del solicitante.

Queda prohibido manipular cualquier tipo de alimentos y bebidas o fumar cerca de los bienes informáticos.

Es atribución exclusiva del personal de la Unidad de Tecnologías y Gestión de la Información, mover, abrir, desconectar o modificar, los equipos de cómputo, periféricos y accesorios propiedad de la Secretaría.

Se prohíbe a los usuarios intercambiar dispositivos (monitores, teclados, mouse, no breaks, reguladores, etc.) de una computadora a otra; dichas modificaciones deberán ser solicitadas a la Unidad de Tecnologías y Gestión de la Información, para que personal autorizado de la unidad en mención realicen los cambios en cuestión.

En caso de que, por asuntos laborales, se requiera extraer de las instalaciones de la Secretaría de Seguridad y Protección Ciudadana, el equipo informático que le fue asignado, deberá solicitar autorización al mando superior inmediato y al titular de la Unidad de Tecnologías y Gestión de la Información.

En caso de que, el equipo informático presente alguna falla o anomalía, el resguardante, deberá reportar por escrito a la Unidad de Tecnologías y Gestión de la Información.

La intervención de terceros en la inspección o mantenimiento al equipo de cómputo, quedará bajo la más estricta responsabilidad del usuario, quien se hará cargo de los costos de sustitución o reparación de cualquier daño o extravió de componentes o de los bienes informáticos.

El usuario de bienes informáticos deberá abstenerse de descargar y distribuir archivos de música, videos y similares con fines no laborales en los equipos informáticos.

Está prohibido usar los equipos asignados para enviar mensajes de amenaza o acoso a los usuarios de la Dependencia o externos.

El personal de soporte tecnológico, está autorizado para acceder a archivos individuales o datos cada vez que deban realizar mantenimiento, reparación o chequeo de equipos de cómputo, y tendrá la facultad de eliminar archivos innecesarios, que degraden el buen funcionamiento del equipo o que no estén autorizados (software no autorizado, archivos de imagen, música y video).

De los Programas de Cómputo (Software)

Los equipos informáticos, únicamente podrán tener instalado el software y aplicaciones que cuenten con licencia, previamente estandarizados y/o autorizados por la Unidad de Tecnologías y Gestión de la Información.

El usuario deberá abstenerse de instalar y/o desinstalar software, incluyendo los de "dominio público" o de "distribución libre", desde y hacia cualquier equipo informático institucional, borrar archivos del sistema o cambiar configuraciones preestablecidas, en caso de ser necesario deberá solicitar dichos cambios a la Unidad de Tecnologías y Gestión de la Información.

Cualquier software o aplicación instalado en un equipo informático, que no cumpla con lo estipulado anteriormente, será desinstalado, sin previo aviso y sin que ello origine ninguna responsabilidad al personal de la Unidad de Tecnologías y Gestión de la Información.

El usuario que no cumpla con el uso correcto del software será acreedor a las sanciones que determine la instancia correspondiente, de conformidad con la normatividad aplicable a la Secretaría de Seguridad y Protección Ciudadana.

Del acceso y Uso de los Sistemas

El uso de los servicios informáticos como acceso a sistemas, red interna de datos, internet y otros, deberán ser solicitados por escrito con visto bueno del superior jerárquico inmediato a la Unidad de Tecnologías y Gestión de la Información, la cual, determinará previo análisis, la autorización, asignación y configuración de direcciones IP, política de control de acceso a la información, perfiles de usuario, filtros WEB y control de aplicaciones correspondientes.

No está permitido el acceso a información o archivos de otros usuarios de la misma u otras áreas, sin permiso o autorización de los mismos, salvo requerimiento por escrito del jefe de área inmediato o por decisión de los mandos medios y superiores de la Secretaría de Seguridad y Protección Ciudadana.

El usuario deberá abstenerse de acceder a los sistemas de información, servicios y bases de datos para los cuales no le fueron otorgados permisos.

El encargado (a) del diseño y/o mantenimiento del sitio web o WEBMASTER, que manipule información referente a la Secretaría de Seguridad y Protección Ciudadana, debe apegarse a las políticas de esta misma Institución, incluyendo derechos de autor, abstenerse de usar software no licenciado.

Del Equipo de Cómputo Externo

El equipo informático que no pertenezca a la Secretaría de Seguridad y Protección Ciudadana, que, por necesidades del servicio y situaciones extraordinarias del personal, se requiera utilizar para coadyuvar con el flujo de trabajo dentro de la misma, deberá contar con

la autorización del Titular de la Unidad de Tecnologías y Gestión de la Información, previo análisis, visto bueno del superior jerárquico y solicitud por escrito.

El usuario de equipo informático externo, que cuente con la autorización correspondiente de uso en la Institución, requiera de los recursos de red oficiales, deberá solicitar por escrito a través de su superior jerárquico, el uso de la red en comento, a la Unidad de Tecnologías y Gestión de la Información; en caso de ser autorizada la solicitud, estará sujeto a las políticas de control de acceso a la información, filtros web y control de aplicaciones, con el objetivo de minimizar los incidentes de seguridad.

De la Seguridad de la Información

La Unidad de Tecnologías y Gestión de la Información realizará de forma constante y perpetua el monitoreo de red y sistemas, con la finalidad de identificar vulnerabilidades, violaciones de seguridad, detección de comportamientos sospechosos o identificación de tráfico anómalo, entre otras, y poder tomar las medidas necesarias para evitar que se produzca un ataque o incidente de seguridad, dentro de las cuales se encuentran:

a. Bloquear y/o desconexión sin previo aviso de toda comunicación de red del equipo de cómputo o dispositivo, con el propósito de minimizar la propagación del malware o mitigar el ataque de seguridad informática.

b. Análisis para determinar el origen del incidente de seguridad, la existencia de información comprometida, la determinación de responsabilidades y las medidas que serán necesarias implementar para que ese incidente específico no ocurra nuevamente.

c. Escaneo y eliminación del software malicioso.

d. Formateo y reinstalación de sistema operativo y demás softwares.

e. Recuperación de la información comprometida en la medida de lo posible.

La Unidad de Tecnologías y Gestión de la Información, en cumplimiento a las directivas de la Secretaría de Seguridad y Protección Ciudadana, determinará los estándares para los contenidos considerados como oficiales para uso laboral, así como, los necesarios para su desempeño. Cualquier otra página o sitio web puede ser bloqueado sin previo aviso al usuario.

Es responsabilidad de los usuarios mantener buenas prácticas de seguridad en el uso de internet, los equipos de cómputo, periféricos y dispositivos USB, para minimizar el riesgo de ejecución de cualquier software malicioso (virus, troyanos, gusanos, adware, spyware, dialers, keyloggers, rootkits o PUPS).

Queda prohibida la instalación o uso de software de espionaje, monitoreo de tráfico de red o programas maliciosos que originen violaciones a la seguridad, interrupción de comunicaciones, intercepción o evasión la autenticación del usuario (inicio de sesión) por cualquier método o que busquen acceder a recursos a los que no se les ha permitido expresamente el acceso.

No está permitido, el uso de herramientas de acceso remoto sin la autorización del jefe inmediato.

No está permitido, el uso de los equipos informáticos, servicios y red de datos para propagar de forma intencional cualquier software malicioso.

Queda prohibido atentar o intentar vulnerar los sistemas de protección o seguridad de red, exceptuando al personal autorizado de la Unidad de Tecnologías de la Información con fines de detección de vulnerabilidades.

No está permitido usar software de navegación anónima y/o proxys con la finalidad de evadir la seguridad y restricciones asignadas a cada usuario.

No está permitido acceder a internet con fines de lucro o recreativos (minería de criptomonedas, apuestas, ventas, publicidad, juegos, chats, radio por internet, servicios de streaming, música y otros).

El usuario deberá evitar actividades que degraden el ancho de banda de la conexión de internet Institucional, como descargas de archivos musicales, imágenes, videos y otros, así como, el uso de radio o video en línea, a menos que sus actividades laborales así lo requieran.

No es permitida la contratación o el uso de dispositivos particulares de acceso a internet (banda ancha móvil, módems, routers, enlaces de microondas y otros) dentro de la Secretaría de Seguridad y Protección Ciudadana, sin la autorización previa del superior jerárquico y la Unidad de Tecnologías y Gestión de la Información.

La contratación de servicios de internet independientes (Modems, bandas anchas y otros) podrán solicitarse a la Coordinación de Administración siempre y cuando cumplan con los siguientes requisitos:

a. Previa solicitud del servicio de internet Institucional a la Unidad de Tecnologías y Gestión de la Información, ésta determine la imposibilidad de brindar el servicio requerido.

b. Se trate de áreas foráneas pertenecientes a la Dependencia y que la Unidad de Tecnologías y Gestión de la Información, haya determinado incosteable o inviable establecer conexiones de cobre, fibra óptica o microondas para brindarles el servicio de intranet e internet Institucional.

c. Se trate de solicitudes de áreas extremadamente críticas para la operatividad de la Dependencia, para las cuales, la Unidad de Tecnologías y Gestión de la Información, determine viable la contratación de un servicio de acceso a internet alternativo, en el supuesto de falla en la red institucional.

Queda prohibido instalar puntos de acceso inalámbricos que se encuentren fuera de la administración y supervisión de la Unidad de Tecnologías y Gestión de la Información, o configurar los equipos de cómputo como zonas con cobertura inalámbrica móvil, con la finalidad de compartir internet, ya que estas acciones representan un riesgo a la seguridad de la información.

El usuario de bienes informáticos, deberá abstenerse de imprimir información confidencial y extraerla de la Secretaría de Seguridad y Protección Ciudadana, con la finalidad de publicarla o manipularla.

El correo electrónico oficial, debe usarse de manera profesional, evitando el envío de información a destinatarios dudosos o desconocidos, la difusión de spam, imágenes y/o videos obscenos e inmorales y cadenas de correos ajenos al ámbito laboral, así como, el uso de identidades falsas y comunicaciones fraudulentas que originen daños a la imagen de la Secretaría de Seguridad y Protección Ciudadana.

De las Sanciones

En observancia a las disposiciones contenidas en el Reglamento de Ética y Disciplina de la Secretaría de Seguridad y Protección Ciudadana y demás normas jurídicas aplicables a la Secretaría de Seguridad y Protección Ciudadana, todos los integrantes de ésta, cualquiera que sea su jerarquía tendrá la obligación de sujetar su actuación con los principios contemplados en estos.

Ahora bien, en los casos en que la o el funcionario público incurra en faltas, omisiones o delitos en manejo de los equipos informáticos y sus componentes, previstos en el presente Manual, la Unidad de Tecnologías y Gestión de la Información, está obligada a dar vista al Órgano Prosecutor de la Unidad de Asuntos Internos, para deslindar responsabilidades.

AUTORIZACIONES Y ACUERDOS

Los lineamientos contemplados en el Manual de Políticas de Tecnologías de la Información de la Secretaría de Seguridad y Protección Ciudadana Políticas, aplican al personal operativo y administrativo de la Secretaría de Seguridad y Protección Ciudadana.

El titular de la Unidad de Tecnologías y Gestión de la Información, en el ámbito de su competencia transmitirá las directrices, parámetros y políticas de control, para que los integrantes de la Secretaría, de una manera clara, precisa y transparente, conozcan y cumplan con el uso adecuado de los bienes informáticos, sujetando su actuación conforme

a los principios que nos rigen, de conformidad con el artículo 3, del Reglamento de la Comisión de Honor y Justicia de la Secretaría de Seguridad y Protección Ciudadana, por ende, está obligado a difundir la información a todas y cada una de las áreas que conforman la Secretaría para conocimiento y debido cumplimiento.

La vigencia del presente Manual de Políticas de Tecnologías de la Información de la Secretaría de Seguridad y Protección Ciudadana, comenzará a correr a partir de la firma del acuerdo.

Dado en la Secretaría de Seguridad y Protección Ciudadana, con residencia en Libramiento Sur Oriente S/N Km. 9, col. Castillo Tielmans, en la ciudad de Tuxtla Gutiérrez, Chiapas; a 06 del mes de noviembre del año dos mil veintitrés; firman al margen y al calce, los servidores públicos siguientes:

Comisaria General Lic. Gabriela del Socorro Zepeda Soto
Secretaria de Seguridad y Protección Ciudadana

Vo. Bo.

Comisario Jefe C.P. Antonio Torres Díaz
Coordinador de Administración

Elaboró

Comisario Lic. Carlos César Gutiérrez Durán
Jefe de la Unidad de Tecnologías y Gestión de la Información

Validó

Comisario Lic. Verónica Campos Escobar
Jefa de la Unidad de Apoyo Jurídico