Secretaría de Cultura y Turismo
Unidad de Información, Planeación, Programación y Evaluación
Departamento de Tecnologías de la Información

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN E INFORMÁTICOS EN CADA UNA DE LAS UNIDADES ADMINISTRATIVAS DE LA SECRETARÍA DE CULTURA Y TURISMO.

Noviembre 2024

CONTENIDO

Marco Legal.

I. Ley de Gobierno Digital del Estado de México y Municipios.

II. Código Administrativo del Estado de México.

III. Código de Procedimientos Administrativos del Estado de México.

IV. Reglamento Interior de la Secretaría de Cultura y Turismo.

V. Reglamento de la Ley que Regula el Uso de Tecnologías de la Información y Comunicación para la Seguridad Pública del Estado de México.

VI. Reglamento de la Ley de Gobierno Digital del Estado de México y Municipios.

VII. Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

VIII. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

IX. Ley de Responsabilidades Administrativas del Estado de México y Municipios.

X. Ley de Documentos Administrativos e Históricos del Estado de México.

XI. Ley de Archivos y Administración de Documentos del Estado de México y Municipios.

XII. Ley Orgánica de la Administración Pública del Estado de México.

GLOSARIO.

Activos: A la información relacionada con el tratamiento de la misma que tenga valor para la Secretaría.

Activos informáticos: A los recursos de software y hardware con los que cuenta la Secretaría, así como la infraestructura tecnológica y todos los elementos que componen el proceso de comunicación, desde la información, el emisor, el medio de transmisión y receptor.

Activos de información: A los recursos de Información que son esenciales o críticos para la operación y objetivos propuestos por la Secretaría y que por su importancia deben ser protegidos conforme al valor que representen.

Alfabeto-Fonético: Al conjunto de palabras usadas por usuarios para deletrear en transmisiones por radio o teléfono para evitar que se produzcan errores de comprensión.

Alfanuméricas: Al término formado por letras y números conjuntamente, las letras pueden ser mayúsculas o minúsculas.

Antivirus: Al software creado con el objetivo de detectar y eliminar virus informáticos como: malware, spyware, troyanos, etc.

Bloqueo: A los mecanismos para evitar el acceso a dispositivos no autorizados que representen un riesgo.

Centro de Datos: Al espacio donde se concentran conectados, todo tipo de servidores para el procesamiento de la información de la Secretaría.

Código Abierto (Open Source): A la creación, programación y desarrollo de servicios, dentro de las instalaciones de la Secretaría.

Código Fuente: Al código de un programa desarrollado por la Secretaría o por terceros.

Confidencialidad: A la propiedad que indica que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Enlace: Al medio de conexión entre dos lugares para ofrecer servicio de internet, video, voz y datos de forma segura para las Unidades Administrativas de la Secretaría.

Extraoficial: A la forma de hacer uso de las cuentas de correo electrónico personales, con la autorización correspondiente.

Fibra Óptica: Al medio de transmisión de comunicaciones telefónicas, de voz y datos a gran velocidad y distancia, sin necesidad de utilizar señales eléctricas instaladas en los diferentes inmuebles pertenecientes a la Secretaría.

Hardware: Al total de los elementos materiales, tangibles que forman parte de un equipo informático.

Inobservancia: Al incumplimiento a las disposiciones cometidas por Servidoras y Servidores Públicos adscritos a la Secretaría.

Intransferible: A las credenciales, cuentas de acceso, claves telefónicas, cuentas de correo institucional o servicios que no pueden transferirse a terceras personas.

Integridad: A la propiedad de salvaguardar la exactitud de la información para que esté completa y sin alteraciones.

Mantenimiento Correctivo: A aquel que corrige los defectos observados en los equipos o instalaciones de la Secretaría.

Mantenimiento Preventivo: A la conservación de equipos informáticos e instalaciones de la Secretaría, mediante la revisión y limpieza que garanticen su buen funcionamiento y fiabilidad.

Mesa de Servicio: Al área destinada a la alta, seguimiento y conclusión de reportes de usuarios de la Secretaría, en materia de Tecnologías de la Información.

Perfiles: A los atributos personalizados, específicamente para los usuarios de la Secretaría.

Personal de Enlace: A las Servidoras y Servidores Públicos designados para apoyar en la difusión e implementación de las Políticas y Lineamientos de Seguridad de la Información en la Secretaría.

Radiocomunicación: A la forma de comunicación usada por los usuarios a través de ondas de radio, mediante protocolos establecidos por la Secretaría.

Redes Inalámbricas: A la conexión de nodos que se da por medio de ondas electromagnéticas, situadas en las instalaciones de la Secretaría, con accesos limitados.

Respaldo: A la copia de seguridad de información realizada en periodos de tiempo determinado, teniendo control para su acceso.

Secretaría: A la Secretaría de Cultura y Turismo del Estado de México.

Servidores de respaldo: A las computadoras con alta capacidad de almacenamiento.

Sistema Operativo: Al software principal de un equipo de cómputo.

Servidores Públicos: A las personas que desempeñen un empleo, cargo o comisión adscritas a la Secretaría.

Sites: Al espacio para albergar equipos de telecomunicaciones y cómputo de la Secretaría, monitoreados las 24 horas para garantizar la integridad de la información.

Software: Al soporte lógico de cualquier sistema informático; es la contraposición a los componentes físicos (hardware).

Software libre: Al programa informático cuyo código fuente puede ser estudiado, modificado, y utilizado libremente, autorizado para su uso en la Secretaría cumpliendo con las medidas de seguridad.

Telecomunicaciones: A toda transmisión y recepción de señales electromagnéticas, gestionadas por las Unidades Administrativas de la Secretaría.

Telefonía Móvil: A la telefonía celular a través de un medio de comunicación inalámbrico proporcionado a personal autorizado adscrito a la Secretaría.

Unidades Administrativas: A las áreas que forman parte de la estructura organizacional de la Secretaría y que están referenciadas en el Reglamento Interno de la Secretaría y el Manual de Organización de la Secretaría.

URL: A la dirección específica que se les asigna a los sistemas informáticos institucionales de la Secretaría.
Videoconferencia: A la Comunicación de audio y vídeo, que permite mantener reuniones con grupos de personas situadas en lugares alejados entre sí, utilizada por las Unidades Administrativas de la Secretaría.

VPN: A la Red Privada Virtual para proporcionar servicios de conexión a través de un canal seguro.

Vulnerabilidad: A los riesgos que un sistema o activo pudiera presentar frente a eventualidades inminentes, dentro de la Secretaría.

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN E INFORMÁTICOS DE LAS UNIDADES ADMINISTRATIVAS DE LA SECRETARÍA DE CULTURA Y TURISMO

Objetivo:	Establecer los lineamientos que permitan salvaguardar la información y la infraestructura informática de la Secretaría, así como garantizar la continuidad de los servicios que se ofrecen. Establecer el instrumento normativo en materia de Seguridad de la Información en las Unidades Administrativas de la Secretaría, para fortalecer la protección de los activos de información e informáticos, promover su buen uso y aplicar medidas de contención de gasto público.
Alcance:	Las presentes Políticas de Seguridad y Control de las Tecnologías de la Información, se deberán observar de manera obligatoria por todos los usuarios de la Secretaría.
Beneficios:	La protección de los activos tecnológicos y de información de la Secretaría
Sanciones por Incumplimiento	La inobservancia de las Servidoras y Servidores Públicos a lo establecido en el presente documento y demás disposiciones aplicables en la materia, será sancionada administrativa y/o penalmente por las autoridades facultadas para sustanciar el procedimiento administrativo y/o penal respectivo, en los términos de la Ley de Responsabilidades Administrativas del Estado de México y Municipios y demás normatividad vigente aplicable en la materia.
Desarrollo e Implementación	El Departamento de Tecnologías de la Información, se coordinará con las Unidades Administrativas de la Secretaría, quienes nombrarán al personal de enlace que fungirá como apoyo para la implementación de las Políticas y Lineamientos de Seguridad de la Información, así como de la supervisión y actualización de las mismas.

POLITICAS DE CLASIFICACIÓN DE LA INFORMACIÓN

PS-CI-001	Los titulares de las Unidades Administrativas de la Secretaría previa consulta con el Comité de Transparencia de la Secretaría, serán responsables de clasificar la información a su alcance de acuerdo con las funciones asignadas, para mantener la confidencialidad, disponibilidad e integridad de ésta, independientemente que se encuentre en formato físico o digital, facilitando su control, manejo y preservación. Los titulares de las Unidades Administrativas que conforman la Secretaría clasificarán los activos de información de acuerdo con los siguientes criterios: **Confidencialidad.**

a) Información pública: Cuando sea de uso general, que por su contenido o contexto no requiere de protección especial y su distribución ha sido permitida a través de canales autorizados por la Institución.

b) La información pública deberá ser de libre acceso, publicarse y difundirse de manera universal, permanente y actualizada en sus formatos físico, o digital.

c) Información reservada: Cuando deba restringirse conforme a los criterios de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

d) Información confidencial: Conforme los criterios que la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios tenga establecidos.

Integridad.

Se consideran cuatro niveles para la clasificación:

a) Alta: Información cuya pérdida ocasionaría un gran impacto en la operación de la Unidad Administrativa.

b) Media: Información cuya pérdida representaría retraso en la operación de la Unidad Administrativa.

c) Baja: Información cuya pérdida ocasiona un impacto no significativo en la operación de la Unidad Administrativa.

d) No clasificada: Información que aún no ha sido clasificada o que está en ese proceso.

Disponibilidad.

Se consideran tres niveles para la clasificación:

a) Alta: La no disponibilidad de la información puede conllevar un impacto en la operación de la Unidad Administrativa.

b) Media: La no disponibilidad de la información puede conllevar a un retraso en la operación de la Unidad Administrativa.

c) Baja: La no disponibilidad de la información puede afectar en lo mínimo la operación de la Unidad Administrativa.

PS-CI-002 Se evitará el acceso, distribución, comercialización, publicación y difusión general de la información, con excepción de las autoridades competentes que, conforme a la ley, tengan acceso a ella y de los particulares titulares de dicha información

PS-CI-003 **Manejo de la información documental**
La información será tratada de acuerdo con su clasificación.

Las Servidoras y Servidores Públicos deberán tener acceso a la información que les permita realizar su trabajo y estarán comprometidos con el uso responsable de ésta.

Los titulares de las Unidades Administrativas implementarán métodos y medidas para administrar, organizar y conservar de manera homogénea los documentos de archivo que reciban, produzcan, obtengan, adquieran, transformen o posean, derivado de sus facultades, competencias, atribuciones o funciones.

Los titulares de las Unidades Administrativas serán los responsables de instrumentar procesos sistematizados que disminuyan el uso de papel en los trabajos de impresión y fotocopiado, en cumplimiento a las Medidas de Austeridad y Contención al Gasto Público del Poder Ejecutivo del Gobierno del Estado de México.

Los titulares de las Unidades Administrativas serán los responsables de gestionar la disponibilidad, localización expedita, integridad y conservación de los documentos del archivo físico.

Los titulares de las Unidades Administrativas serán corresponsables en el uso de la información documental. Las Servidoras y Servidores Públicos evitarán dejar documentación dentro de los dispositivos de impresión, fotocopiado o digitalización.

PS-CI-004 **Manejo de la información electrónica y digital.**
Se deberá tratar la información de acuerdo con su clasificación.

Las Servidoras y Servidores Públicos deberán tener acceso a la información que les permita realizar su trabajo y estarán comprometidos con el uso responsable de ésta.

Las Servidoras y Servidores Públicos deberán garantizar que los documentos de archivo electrónico o digital posean las características de confidencialidad, integridad y disponibilidad, con la finalidad de que gocen de la validez de un documento original.

Los titulares de las Unidades Administrativas deberán etiquetar la información indicando su tipo de clasificación para facilitar su control, manejo y cuidado por parte del personal.

Los titulares de las Unidades Administrativas procurarán establecer una nomenclatura estándar para el manejo de carpetas y archivos electrónicos.

Los titulares designarán a las Servidoras y Servidores Públicos responsables para el manejo de la información electrónica y digital.

PS-CI-005 **Inventario de activos de información.**

Los titulares de las Unidades Administrativas una vez que han realizado la clasificación y etiquetado de los activos de información, remitirán al Departamento de Tecnologías de la Información, la documentación soporte en formato electrónico para integrar los datos al inventario de activos de información.

Es responsabilidad de los titulares de las Unidades Administrativas, a través de las Servidoras y Servidores Públicos que designe el informar los cambios de clasificación, baja o alta de nuevos activos al Departamento de Tecnologías de la Información, a fin de actualizar el inventario.

POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS

PS-RH-001 Los titulares de las Unidades Administrativas de la Secretaría establecerán las reglas que las Servidoras y Servidores Públicos deberán observar ante los movimientos de personal relacionados con el manejo de activos y activos informáticos, que permitan garantizar la confidencialidad y el uso responsable de la información generada en la Secretaría.

Difusión de las Políticas de Seguridad de la Información

Los titulares de las Unidades Administrativas con el apoyo del Personal de Enlace serán los responsables de fomentar la difusión de las Políticas y Lineamientos de Seguridad de la Información hacia las Servidoras y Servidores Públicos de nuevo ingreso a la Secretaría.

Las Servidoras y Servidores Públicos serán los responsables de aplicar en su entorno laboral, las Políticas y Lineamientos de Seguridad de la Información.

Las Servidoras y Servidores Públicos de la Secretaría estarán obligados a informar a su jefe inmediato las posibles vulnerabilidades detectadas en la Seguridad de la Información.

PS-RH-002 **Protección de la información**

Las Servidoras y Servidores Públicos que, por asignación del cargo o comisión, administren, capturen, consulten, recaben o transfieran información, estarán obligados a salvaguardarla y conservarla, a fin de cumplir con los criterios de confidencialidad, integridad y disponibilidad.

Las Servidoras y Servidores Públicos firmarán un acuerdo de confidencialidad de la información, el cual se revisará periódicamente.

PS-RH-003 **Cambio de funciones.**
En el caso de cambios de adscripción o asignación de nuevas funciones, los titulares de las Unidades Administrativas o en su caso el Área Administrativa, serán los responsables de definir

las acciones para la entrega del cargo de las Servidoras y Servidores Públicos, evitando la sustracción de información relacionada con el puesto que ocupaban

PS-RH-004 **Conclusión de la relación laboral.**
Las Servidoras y Servidores Públicos al concluir su relación laboral con la Secretaría dejarán de conservar en su poder los activos y activos informáticos, que por motivos del cargo o funciones tenían bajo su resguardo, lo cual quedará asentado en un documento o bien en el acta de los sujetos obligados a la Entrega y Recepción.

POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL

PS-FA-001 Los titulares de las Unidades Administrativas establecerán controles de acceso físico a sus instalaciones y conservarán espacios de trabajo libres de interferencias para prevenir daños a la infraestructura tecnológica, evitando así, poner en riesgo la seguridad de la información y la continuidad de la operación.

Acceso físico a oficinas e instalaciones.
Los titulares de las Unidades Administrativas, establecerán medidas de control de acceso a sus instalaciones, tanto en áreas comunes como en áreas restringidas. Las Unidades Administrativas que albergan infraestructura tecnológica crítica, deberán ser consideradas de acceso restringido.

Las Servidoras y Servidores Públicos que cumplan sus funciones en oficinas o despachos, las cerrarán con llave al final de la jornada laboral.

Los titulares de las Unidades Administrativas instruirán la utilización de la identificación oficial visible para las Servidoras y Servidores Públicos, así como para terceros.

Los titulares de las Unidades Administrativas a través de las Servidoras y Servidores Públicos que ellos designen restringirán o supervisarán el ingreso de dispositivos de almacenamiento externo, así como de audio y video.

Los titulares de las Unidades Administrativas a su consideración fomentarán la restricción cuando por motivo de la sensibilidad de la información se justifique, el uso de dispositivos electrónicos en las áreas laborales.

Los titulares de las Unidades Administrativas establecerán controles documentales de acceso físico, tales como bitácoras de acceso a las instalaciones, los cuales se revisarán periódicamente.

PS-FA-003 **Seguridad de la infraestructura.**

Los titulares de las Unidades Administrativas, establecerán mecanismos de protección de la infraestructura tecnológica que las Servidoras y Servidores Públicos tengan asignada para desempeñar sus labores, atendiendo los siguientes lineamientos:

Los equipos de cómputo no deberán estar expuestos a la luz solar por tiempos prolongados.

Deberán mantener despejadas las áreas de ventilación donde se ubique la infraestructura tecnológica.

La infraestructura tecnológica sólo podrá ser reubicada por el personal técnico autorizado por el Departamento de Tecnologías de la Información.

Las Servidoras y Servidores Públicos evitarán comer o beber en el espacio de trabajo.

Los activos informáticos que se encuentren conectados a las tomas de corriente regulada deberán estar protegidos contra cualquier variación de voltaje, para ello se atenderán las siguientes indicaciones

Las tomas de corriente a las que se conecten los activos informáticos permanecerán siempre en buenas condiciones, por lo tanto, las Servidoras y Servidores Públicos que detecten fallas o defectos, deberán reportarlo a su jefe inmediato.

Los titulares de las Unidades Administrativas supervisarán que no se conecten a las tomas de corriente regulada destinadas para los activos informáticos o cualquier aparato eléctrico que genere variación de voltaje.

El mantenimiento preventivo y correctivo de los activos informáticos de la Secretaría, se solicitará al Departamento de Tecnologías de la Información.

Las Servidoras y Servidores Públicos de las Unidades Administrativas la Secretaría, estarán impedidos para manipular o modificar el estado de los activos informáticos.

La reubicación de los activos informáticos únicamente se efectuará por el personal del Departamento de Tecnologías de la Información, a través del área de Soporte Técnico.

El Personal de Enlace de cada Unidad Administrativa inspeccionará la entrada y salida de los activos informáticos en las instalaciones de la Secretaría.

Las Servidoras y Servidores Públicos serán responsables de los activos informáticos que tengan bajo su resguardo, dentro y fuera de las instalaciones.

Los titulares de las Unidades Administrativas supervisarán que las Servidoras y Servidores Públicos mantengan sus espacios de trabajo, libre de objetos que no correspondan a sus actividades laborales.

Al ausentarse de su espacio de trabajo, las Servidoras y Servidores Públicos cuando el mobiliario y el espacio físico así lo permitan, evitarán dejar documentos que contengan información institucional a la vista.

Las Servidoras y Servidores Públicos mantendrán bloqueados sus equipos de cómputo cuando no se encuentran en su lugar de trabajo.

POLÍTICAS DE SEGURIDAD EN LA OPERACIÓN.

PS-O-001 El Departamento de Tecnologías de la Información, designará a los responsables de la operación de los activos de información e informáticos, para coordinar que el uso adecuado, mantenimiento y actualización de estos, sean controlados y documentados, minimizando riesgos en los activos referidos y protegiendo la información.

PS-O-002 **Responsabilidades y procedimientos de operación**
El Departamento de Tecnologías de la Información regulará los procedimientos de operación de los activos de información e informáticos de las Unidades Administrativas de la Secretaría, verificando que se realicen conforme a los lineamientos establecidos.

El Departamento de Tecnologías de la Información será responsable de supervisar que los procedimientos de operación de sus activos de información e informáticos cuenten con la documentación técnica respectiva.

PS-O-003 Controles contra el código malicioso.
El Departamento de Tecnologías de la Información a través del Área de Soporte Técnico, será responsable de realizar y supervisar:

- La instalación de software en los activos informáticos.
- La realización periódica de un escaneo en los equipos de cómputo, con el fin de verificar que no exista código malicioso.
- La permanencia de las configuraciones de seguridad para reducir el riesgo de virus en las aplicaciones y uso de navegadores.
- La instalación de antivirus en los equipos de cómputo.

PS-O-004 **Copia de seguridad.**
La información será respaldada independientemente de su clasificación, en los medios de almacenamiento que los titulares de las Unidades Administrativas autoricen, incluyendo dispositivos de almacenamiento externo.

Los titulares de las Unidades Administrativas supervisarán que se generen respaldos de información en periodos de tiempo determinados, según el procedimiento establecido y de acuerdo a la clasificación de la información que tengan bajo su resguardo.

Los titulares de las Unidades Administrativas implementarán un registro (bitácora) de los respaldos generados, que contenga la siguiente información:

- Número de folio o consecutivo del respaldo.

- Fecha de respaldo.
- Hora de respaldo.
- Unidad Administrativa.
- Titular de la Unidad Administrativa.
- Área que genera la información.
- Nombre del responsable que realizó el respaldo.
- Nombre del jefe inmediato.

El personal designado por los titulares de las Unidades Administrativas verificará que la información respaldada, al ser restaurada se conserve integral.

PS-O-005 **Registro de actividades y supervisión.**

El Departamento de Tecnologías de la Información supervisará que las Servidoras y Servidores Públicos que utilicen una cuenta interna con acceso a aplicativos, información confidencial, consolas de operación y servidores de cómputo, ubicados en las instalaciones de la Secretaría, accedan únicamente a los activos informáticos que tienen permitido.

El Departamento de Tecnologías de la Información aplicará los mecanismos necesarios para que las contraseñas de las Servidoras y Servidores Públicos para el acceso a aplicativos sean tratadas como sensibles y confidenciales.

La información que sea ingresada a los sistemas institucionales tendrá que ser supervisada por la Unidad Administrativa usuaria y por el Departamento de Tecnologías de la Información

PS-O-006 **Uso de software.**

La instalación de software de cualquier tipo será realizada estrictamente por personal el Departamento de Tecnologías de la Información previa solicitud de los titulares de las Unidades Administrativas.

Todo software utilizado dentro de la Secretaría deberá contar con una autorización para su uso.

El software que se tenga instalado en cada equipo de cómputo corresponderá a las funciones y actividades que se realizan de acuerdo con las atribuciones de la Unidad Administrativa.

Se considerará el uso de software libre siempre y cuando cumpla con las medidas de seguridad lógica que se tengan establecidas.

Se evitará el uso de software libre en equipos que alojen sistemas de aplicaciones productivas, y que represente un riesgo para la seguridad de la información.

PS-O-007 **Gestión de vulnerabilidad técnica**

Las Servidoras y Servidores Públicos autorizados obtendrán acceso a la infraestructura de red y activos informáticos, como son:

- Centro de Datos.
- Servidores de Respaldos.

- Bases de Datos.

El Departamento de Tecnologías de la Información, establecerá mecanismos para proteger la información contra la acción de agentes externos o vulnerabilidades locales.

Las licencias y paquetes de software deberán ser resguardados por la el Departamento de Tecnologías de la Información.

El personal adscrito a las Unidades Administrativas de la Secretaría evitará la divulgación de las rutas de acceso (URL) de los sistemas institucionales, salvo aquellas que sean de acceso público.

Las rutas de acceso (URL) de los sistemas institucionales serán utilizadas únicamente en equipos autorizados por el Departamento de Tecnologías de la Información

Tratándose de activos informáticos arrendados por terceros, el Departamento de Tecnologías de la Información vigilará que los respaldos de información, traslado y sustitución de equipos, así como el mantenimiento preventivo y correctivo se lleven a cabo conforme a las condiciones especificadas en el contrato celebrado con los proveedores respectivos.

POLÍTICAS DE CONTROL DE ACCESOS LÓGICOS

PC-AL-001 El Departamento de Tecnologías de la Información establecerá los mecanismos de acceso y reserva a los activos informáticos generados, y administrados por la Secretaría, que deberán cumplir los usuarios, manteniendo la confidencialidad y el uso responsable de la información.

PC-AL-002 **Gestión de acceso de usuario.**

El Departamento de Tecnologías de la Información definirá un procedimiento para otorgar los accesos a los usuarios autorizados, e impedir los accesos a los no autorizados, asignando los permisos que correspondan, clasificando la información en base a su impacto y considerando la confidencialidad requerida.

Gestión de registro de usuario

El Departamento de Tecnologías de la Información realizará el alta de usuarios de acuerdo al procedimiento establecido, con el objeto de habilitar la asignación de los derechos de acceso a los activos informáticos de la Secretaría.

Gestión de derechos de acceso asignados a usuarios.

El Departamento de Tecnologías de la Información implementará controles para la asignación de acceso a los activos informáticos con perfiles específicos.

Los usuarios deberán tener acceso a la información que les permita realizar sus funciones, haciendo uso responsable de la misma.

Gestión de derechos de acceso con privilegios.

La asignación de privilegios especiales para usuarios deberá ser realizada de acuerdo con la clasificación de la información y los perfiles de acceso, que establezca el Departamento de Tecnologías de la Información.

Gestión de autenticación de usuarios.

El Departamento de Tecnologías de la Información proporcionará a los usuarios, credenciales de acceso personales e intransferibles para el uso de los activos informáticos, las cuales deben identificar y autenticar usuarios, evitando accesos no autorizados.

Revisión de derechos de acceso de los usuarios.

El Departamento de Tecnologías de la Información deberá supervisar periódicamente los derechos de acceso otorgados a los usuarios, mediante monitoreo de actividades y eventos realizados por los usuarios.

Retirada o adaptación de los derechos de acceso.

En caso de ser detectada alguna actividad sospechosa o inusual en la cuenta del usuario que pueda comprometer la integridad o confidencialidad de la información institucional, se suspenderá temporalmente el acceso, y solo será habilitado después de tomar las medidas que considere necesarias el Departamento de Tecnologías de la Información.

Al concluir la relación laboral, o por cambio de adscripción de los usuarios, el Departamento de Tecnologías de la Información, deberá retirar los derechos de acceso a los usuarios o terceros que ya no deban tenerlo.

PC-AL-003

Responsabilidades del usuario.
El conocimiento y cumplimiento de estos lineamientos de seguridad son de carácter obligatorio para los usuarios. Los activos informáticos deberán ser operados bajo los principios de confidencialidad y reserva, realizando un uso adecuado y responsable en los mismos.

a) Uso de contraseñas

Los usuarios deberán aplicar las buenas prácticas de seguridad respecto a la nomenclatura y uso de las contraseñas, considerando las siguientes recomendaciones:

- Las contraseñas se deberán mantener como confidenciales en todo momento.
- Las contraseñas son personales e intransferibles.
- Debe evitarse escribir las contraseñas en papeles de fácil acceso.
- Inhabilitar la opción "recordar clave en este equipo".
- Las contraseñas deberán estar compuestas de una combinación de al menos ocho (8) caracteres alfanuméricos, incluyendo un carácter especial.

- Cambiar su contraseña de manera periódica.
- Cuando se sospeche la violación de la contraseña, el usuario deberá notificarlo de inmediato la Mesa de Servicio.
- Cuando el usuario olvide, bloquee o extravíe sus contraseñas deberá reportarlo a la Mesa de Servicio.

b) Equipo informático de usuario desatendido.

El usuario deberá mantener su lugar de trabajo, libre de cualquier información confidencial durante su ausencia, evitando permitir accesos no autorizados en los activos de información e informáticos.

PC-AL-004 **Control de acceso a sistemas operativos y aplicativos.**

El Departamento de Tecnologías de Información, deberá garantizar el acceso exclusivo a los usuarios autorizados, implementando estándares de seguridad en sus sistemas y aplicativos que minimicen la divulgación, modificación, sustracción o intromisión en los activos de información e informáticos.

a) Restricción de acceso a la información.

Los activos informáticos serán tratados con reserva y confidencialidad de acuerdo a la clasificación otorgada; únicamente los usuarios autorizados tendrán acceso a ellos, de acuerdo a las funciones que desempeñen.

b) Procedimientos seguros de inicio de sesión.

Es obligatorio que los activos informáticos utilizados por las Unidades Administrativas de la Secretaría, cuenten con mecanismos de autenticación en el acceso de los mismos.

Para ello el Departamento de Tecnologías de la Información

- Establecerá controles de autenticación, que eviten la visualización de contraseñas.
- Implementará controles que detecten múltiples intentos de autenticación fallida.
- Implementará controles que obliguen al usuario a cambiar la contraseña por defecto en el primer ingreso.

c) Gestión de contraseñas de usuario.

La administración de usuarios y contraseñas se deberá realizar por medio de procedimientos formales de gestión a cargo del Departamento de Tecnologías de la Información, tomando en cuenta lo siguiente:

- Remitir la solicitud con los datos del usuario mediante oficio.

-El usuario y contraseña otorgados deberán tratarse de manera personal y confidencial.

El Departamento de Tecnologías de la Información, realizará la implementación de un inicio seguro de sesión, mediante la asignación de contraseñas predeterminadas para los usuarios, basándose en los criterios siguientes:

- La confidencialidad de la contraseña.
- Validación de los datos de acceso.
- Identificación del número de intentos fallidos de conexión, para bloquear el acceso, si rebasa el máximo permitido.
- Ocultando los datos de la contraseña digitados.

d) Control de acceso al código fuente de los programas.

El Departamento de Tecnologías de la Información, controlará el acceso al código fuente de los programas y sistemas de información desarrollados por la Secretaría, llevando un control de los cambios autorizados y aplicados en el código fuente. Se asegurará que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, estableciendo procedimientos y controles.

Los desarrolladores internos o externos estarán sujetos al acceso controlado y/o limitado a los activos de información e informáticos que se encuentren en los ambientes de producción.

e) Aislamiento de sistemas sensibles.

El Departamento de Tecnologías de la Información, supervisará que los sistemas y activos informáticos sensibles o críticos, dispongan de un entorno informático dedicado (propio), evitando que tengan acceso por vía remota o red, solo se permitirá el acceso presencial en el lugar donde se encuentre dicho activo.

POLÍTICAS DE TELECOMUNICACIONES

PS-TL-001

El Departamento de Tecnologías de la Información, establecerá los mecanismos de uso y operación de las redes y telecomunicaciones, para mantener la confidencialidad de la información que se transmite a los usuarios, a través de las diferentes tecnologías implementadas en la Secretaría.

El lenguaje utilizado por los usuarios del sistema de radiocomunicación de la Secretaría debe estar apegado al respeto, moral y buenas costumbres.

Las Servidoras y Servidores Públicos de la Secretaría y terceros, que sean usuarios del sistema de radiocomunicación, deberán emplear las claves alfanuméricas y el código alfabeto-fonético establecidos para dicho sistema.

Debe evitarse la divulgación de las claves oficiales de la Secretaría y frecuencias de operación

Las Servidoras y Servidores Públicos de la Secretaría, están impedidos para operar radios o frecuencias de otras instituciones o entidades sin la autorización de los titulares de las Unidades Administrativas.

Las Servidoras y Servidores Públicos de la Secretaría deben impedir el uso u operación de los equipos de radiocomunicación a su cargo, a personas no autorizadas.

Las Servidoras y Servidores Públicos de la Secretaría están impedidos de solicitar o dar remuneración alguna, por cualquier atención otorgada mediante los equipos de radiocomunicación.

El uso y cuidado de cada terminal (portátil, móvil o base fija), es responsabilidad única de las Servidoras y Servidores Públicos de la Secretaría a quienes que se les asigna.

Toda falla que presente el sistema, deberá será reportada a la Mesa de Servicio de la Secretaría.

La instalación, desinstalación, configuraciones, mantenimiento preventivo y correctivo de los equipos de comunicación, estará a cargo del Departamento de Tecnologías de la Información

PS-TL-002 **De la telefonía fija**

La clave telefónica será de uso intransferible, los titulares de las Unidades Administrativas informarán al Departamento de Tecnologías de la Información, cualquier cambio o baja de las Servidoras y Servidores Públicos de la Secretaría, a los que se les asignó.

Los equipos de telefonía fija serán distribuidos según los requerimientos del área y funciones asignadas a las Servidoras y Servidores Públicos solicitantes.

Las líneas telefónicas se utilizarán exclusivamente como una herramienta de apoyo a las labores encomendadas, por lo que las llamadas deberán ser breves, utilizando un vocabulario acorde a las buenas costumbres.

La instalación, desinstalación, de los equipos de telefonía, estará a cargo del Departamento de Tecnologías de la Información.

PS-TL-003 **De las redes inalámbricas**

Las Servidoras y Servidores Públicos de la Secretaría y terceros requerirán autorización expresa de los titulares de las Unidades Administrativas, para el acceso a las redes inalámbricas, previa justificación de la solicitud.

Se establecerán procedimientos de autorización y controles para la administración de accesos a las redes inalámbricas, siendo el Departamento de Tecnologías de la Información, el encargado de esta función.

El Departamento de Tecnologías de la Información, creará perfiles para el uso de las redes inalámbricas en las Unidades Administrativas de la Secretaría.

Se verificarán los perfiles de acceso asignado a las Servidoras y Servidores Públicos de la Secretaría, con el fin de revisar que se les permita el acceso a aquellos recursos que les fueron autorizados.

PS-TL-004 **Del Correo electrónico.**

La administración de las cuentas de correo electrónico institucional será llevada a cabo exclusivamente por el Departamento de Tecnologías de la Información de la Información.

La Agencia Digital establecerá controles que permitan garantizar la seguridad de la plataforma de correo electrónico contra código malicioso.
El Departamento de Tecnologías de la Información, concientizará al personal de la Secretaría y terceros en temas de seguridad que deben adoptar para el intercambio de información, por medio del correo electrónico.

Las cuentas de correo electrónico institucional serán de uso individual, intransferible y para uso exclusivo del personal adscrito a la Secretaría.

Para el intercambio de información en actividades laborales, no se permitirá el uso de correos electrónicos no institucionales.

Utilizar las etiquetas de seguimiento en el envío, respuesta o renvío de correos electrónicos institucionales

Las Servidoras y Servidores Públicos y terceros, serán cuidadosos de la información contenida en los buzones del correo, ya que es propiedad de la Secretaría, de igual forma mantendrán en ellos solo la información relacionada a las funciones asignadas.

Las Servidoras y Servidores Públicos y terceros, respetarán el formato establecido en la imagen institucional definidos por la Secretaría; así como conservarán en todos los casos el criterio de confidencialidad, bajo los términos normativos y de transparencia relacionados con el tratamiento de información.

Será responsabilidad de las Servidoras y Servidores Públicos, cerrar su cuenta de correo al dejar de utilizarlo, para evitar que otros usuarios puedan hacer uso de él.

Las Servidoras y Servidores Públicos y terceros, respaldarán la información contenida en su cuenta de correo, o si es el caso, solicitarán al Departamento de Tecnologías de la Información realizar los respaldos.

Las Servidoras y Servidores Públicos de la Secretaría y tomaran medidas pertinentes ante cualquier mensaje de correo de procedencia desconocida o sospechosa, con el fin de evitar posibles infecciones por código malicioso o virus.

Las Servidoras y Servidores Públicos y terceros, reportarán oportunamente al Departamento de Tecnologías de la Información, cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, perdida de contraseña, etc., a fin de poder tomar las medidas pertinentes.

El uso de las cuentas de correo, creadas para las diferentes Unidades Administrativas, que sean compartidas por el personal de éstas, serán responsabilidad de los titulares de las Unidades Administrativas.

Se debe evitar utilizar la cuenta de correo institucional para darse de alta en páginas que sean ajenas a las funciones laborales asignadas, excepto cuando se tenga autorización expresa de los titulares de las Unidades Administrativas.

PS-TL-005 **Del Servicio de Internet**

El Departamento de Tecnologías de la Información, establecerá las configuraciones autorizadas para los dispositivos que hagan uso de los servicios de internet provistos por la Secretaría.

El Departamento de Tecnologías de la Información, otorgará permisos para la navegación a través del servicio de internet, en función de las labores encomendadas a los usuarios, asegurándose de que los equipos que utilicen el servicio, cuenten con software antivirus.

Las Servidoras y Servidores Públicos evitarán hacer uso de servicios de internet público en equipos institucionales.

Utilizar las etiquetas de seguimiento en el envío, respuesta o renvío de correos electrónicos institucionales de las Unidades Administrativas.

PS-TL-006 **De las Redes LAN**

El Departamento de Tecnologías de la Información, establecerá procedimientos de autorización y controles para asegurar los accesos de las redes de datos y los recursos de red disponibles en las Unidades Administrativas adscritas a la Secretaría.

El Departamento de Tecnologías de la Información, otorgará permisos según el perfil y necesidades para el uso de los recursos de red de las Unidades Administrativas de la Secretaría, y será quien brinde el soporte y la atención solicitada en el tema.

El Departamento de Tecnologías de la Información, verificará los permisos de acceso para el personal, con el fin de revisar que tengan autorización únicamente a aquellos recursos de red y servicios de la plataforma tecnológica a los que les fueron asignados.

Las Servidoras y Servidores Públicos y terceros, antes de contar con acceso lógico por primera vez a la red de datos de la Secretaría, deberán contar con el procedimiento de creación de cuentas de usuario debidamente autorizado.

Las Servidoras y Servidores Públicos que se conecten a las redes deberán cumplir con los requisitos o controles para autentificarse en ellas.

El Departamento de Tecnologías de la Información, planeará y desarrollará los proyectos tecnológicos en materia de redes LAN, como parte de los servicios de seguridad de las Tecnologías de Información de la Secretaría.

El Departamento de Tecnologías de la Información evaluará constantemente las diferentes tecnologías en materia de telecomunicaciones, existentes en el mercado con la finalidad de una posible mejora en las redes LAN.

El Departamento de Tecnologías de la Información, quien defina el uso de las redes LAN, y los controles de seguridad asociados, además garantizará los servicios de voz y datos en las Unidades Administrativas de la Secretaría.

El Departamento de Tecnologías de la Información, proporcionará el medio de enlace local para brindar servicios de internet, voz, video y datos de forma segura para las Unidades Administrativas adscritas a la Secretaría.

El Departamento de Tecnologías de la Información, impulsará desarrollar aplicativos tecnológicos en código abierto (open source), para proporcionar servicios confiables y robusto a las Unidades Administrativas adscritas a la Secretaría.

El Departamento de Tecnologías de la Información controlará los equipos de comunicaciones locales, servidores y sites de comunicaciones, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la integridad de la información.

El Departamento de Tecnologías de la Información coordinará el soporte preventivo y correctivo, en materia de comunicaciones, voz, datos, y video, de los servicios de red proporcionados a las Unidades Administrativas que integran la Secretaría.

PS-TL-007 **Redes WAN**

El Departamento de Tecnologías de la Información planeará y desarrollará los proyectos tecnológicos en materia de redes WAN, como parte de los servicios de seguridad de las tecnologías de información y comunicaciones de la Secretaría.

El Departamento de Tecnologías de la Información, evaluará constantemente los procedimientos de trabajo en materia de telecomunicaciones y seguridad de las redes WAN de la Secretaría.

El Departamento de Tecnologías de la Información, será la única que definirá el uso de las redes WAN, así como la seguridad en este medio.

El Departamento de Tecnologías de la Información, garantizará los servicios de voz, video y datos en las Unidades Administrativas de la Secretaría mediante las redes WAN.

El Departamento de Tecnologías de la Información, evaluará la posibilidad de impulsar y desarrollar servicios tecnológicos a través de redes virtuales privadas (VPN), para proporcionar servicios confiables, robustos y con un costo accesible para la Secretaría.

El Departamento de Tecnologías de la Información, controlará los equipos de comunicaciones, servidores y sites de comunicaciones de las redes WAN, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la confidencialidad e integridad de la información.

El Departamento de Tecnologías de la Información, coordinará el soporte técnico preventivo y correctivo en materia de comunicaciones, voz, datos, video y seguridad de las redes WAN de la Secretaría.

El Departamento de Tecnologías de la Información, estará en constante monitoreo de las redes WAN a fin de brindar un servicio confiable y eficaz para los diferentes edificios pertenecientes a la Secretaría.

El Departamento de Tecnologías de la Información, dará aviso al o los proveedores encargados de la infraestructura exterior en caso de cortes o actos vandálicos en antenas de microondas o fibra óptica, que afecten las comunicaciones a nivel WAN entre edificios pertenecientes a la Secretaría.

POLÍTICAS DE LOS USUARIOS

PS-US-001 Todos las Servidoras y Servidores Públicos de la Secretaría, que hagan uso de equipo de cómputo y de los servicios informáticos propiedad o arrendados del Gobierno del Estado de México para el desempeño de sus funciones, deberán cumplir y respetar las presentes Políticas de Seguridad y Control de las Tecnologías de la Información.

PS-US-002 Queda estrictamente prohibido para el usuario:

- Reubicar el equipo de cómputo, comunicación, dispositivos periféricos y dispositivos informáticos en general, sin verificar previamente con el Departamento de Tecnologías de la Información la viabilidad.
- Manipular el hardware y software del equipo de cómputo asignado que utilice para el desempeño de sus funciones para intentar corregir algunas fallas, modificar la configuración o pretenda añadir o retirar algún componente interno.
- Desconectar de la energía eléctrica los dispositivos informáticos (módem, hub, switch, conmutadores, impresoras, scanners etc.).

- Dañar o maltratar los equipos informáticos arrendados y los que son propiedad de la Secretaría.
- Utilizar herramientas o software que alteren, dañen o expongan los controles de seguridad informática.
- Modificar la configuración, infraestructura y servicios de Red de Voz y Red Datos (LAN y WIFI).
- Interferir, manipular o dañar las conexiones y el cableado de la red de Voz y Datos.
- Cubrir los orificios de ventilación del monitor y/o del gabinete del CPU.
- Colocar el equipo en lugares húmedos y sin las condiciones de higiene adecuadas.
- Consumir alimentos o líquidos cerca del equipo de cómputo, toda vez que pueden poner en riesgo los mismo.
- Almacenar y compartir archivos personales en el equipo asignado (documentos, videos, imágenes, audios, juegos, entre otros), toda vez que pueden afectar el funcionamiento de los equipos de cómputo.

La única instancia autorizada para realizar las actividades anteriores es el personal técnico del Departamento de Tecnologías de la Información adscrito a la Unidad de Información, Planeación, Programación y Evaluación de esta Secretaría, o en su caso, los proveedores encargados de atender los servicios de garantía, por las empresas arrendadoras de los bienes informáticos.

PS-US-003

Es obligación de todo el personal adscrito a la Secretaría observar las siguientes recomendaciones:

- Bloquear el acceso a su equipo cuando se ausente de su espacio de trabajo.
- Salvaguardar la confidencialidad de las credenciales de acceso a los diversos sistemas que tengan a bien operar para el desarrollo de sus actividades administrativas.
- Evitar abrir o ejecutar archivos o macros adjuntos de un correo electrónico de procedencia desconocida, sospechosa, fuente no confiable, o ajeno al dominio institucional.
- Evitar el uso de software VPN o emuladores (BitTorrent, Emule, Ares, Utorrent, etc.) para la descarga y transferencia de archivos multimedia, ya que satura el ancho de banda de internet y se propagan todo tipo de ataques informáticos tales como virus, malwares, adwares, entre otros.

- Evitar el uso de los equipos de cómputo para acceder a las redes sociales personales, sitios de ocio y páginas de contenido multimedia.
- Eliminar los correos electrónicos de procedencia desconocida, sospechosa o fuente no confiable y de ser posible reportarlo al Departamento de Tecnologías de la Información.
- Borrar los correos spam o cadenas y no realizar el reenvío de los mismos.
- Descargar archivos de sitios desconocidos o fuentes sospechosas.
- Hacer uso del software antivirus para revisar los discos duros, unidades de almacenamiento removibles o memorias USB antes de usarlas.

PS-US-004	Solo se podrá hacer uso de los bienes informáticos asignados y autorizados de acuerdo con los perfiles establecidos derivado de las funciones o actividades relacionadas con los procesos.
PS-US-005	Los servicios de red, como cuentas de usuario, contraseñas, configuraciones, y cualquier otro tipo de identificador y autenticador, es información estrictamente confidencial y de uso exclusivo
PS-US-006	Para el acceso a sistemas de información, redes internas y/o aplicaciones específicas, se proporcionará un nombre de usuario y contraseña, debiendo firmar el Acuerdo de Confidencialidad.
PS-US-007	Los servicios de comunicación, de acceso a Internet y las cuentas de correo con dominio institucional o comerciales, usadas en el desarrollo de las funciones encomendadas, son de uso oficial y sólo debe ser utilizado para este fin, quedando bajo responsabilidad de cada usuario la información que se manipule en cada una de los equipos.
PS-US-008	Se tiene prohibido el uso del correo institucional para manejo de información ajena a los intereses de la Secretaría.
PS-US-009	Queda prohibida la instalación de software genérico, que no sea con previa autorización del personal de Departamento de Tecnologías de la Información de la información
PS-US-010	Los titulares de las unidades administrativas deberán informar previamente al Departamento de Tecnologías de la Información sobre la des habilitación y/o cambio de cuentas de usuarios de sistemas y/o correo electrónico institucional que han terminado su relación laboral o por motivo de reubicación del personal, para llevar a cabo el cambio de credenciales de acceso correspondiente.
PS-US-011	Observar la correcta utilización de los equipos de cómputo y accesorios asignados, así como de los dispositivos periféricos propiedad de la Secretaría o arrendados del Gobierno del Estado de México que utilice para el desempeño de sus funciones
PS-US-012	Se deberá reportar al personal técnico cualquier falla de los bienes informáticos a través del mecanismo que establezca el Departamento de Tecnologías de la Información.

PS-US-013	Es responsabilidad de los usuarios realizar el respaldo de información y la actualización del equipo de cómputo asignado.
PS-US-014	Para atención de Soporte Técnico especializado se deberá generar un ticket con el Departamento de Tecnologías de la Información en cualquiera de las siguientes opciones: • De manera Presencial: en el Departamento de Tecnologías • Vía electrónica: departamento.tecnologias@edomex.gob.mx • Comunicándose al teléfono: 722 274 1315 con número de ext. 1091 Al levantar una solicitud, se le asignará un folio, el cual será utilizado para dar seguimiento al servicio requerido, una vez concluido, se entregará un formato oficial del Departamento de Tecnologías de la Información que describirá el diagnóstico, las actividades realizadas y en caso de que aplique, los recursos materiales utilizados, el formato dará constancia y validación de la atención brindada mediante la signatura del solicitante en el formato de reporte. Es importante mencionar que, no se brindará atención a solicitudes realizadas a través de medios no oficiales, incluyendo los teléfonos personales del equipo del Departamento de Tecnologías de la Información. Esta medida tiene como objetivo optimizar la gestión de las solicitudes y asegurar una respuesta oportuna y eficiente.
PS-US-015	Queda prohibida la extracción o sustracción de información parcial o total, quedando bajo la responsabilidad directa del usuario el resguardo, integridad y no divulgación de la misma.
PS-US-016	Proteger, organizar y mantener en orden la información contenida en el equipo de cómputo que le ha sido asignado para el desarrollo de sus funciones
PS-US-017	La instalación del Software debe ser autorizada por el jefe de departamento o superior y confirmar que es requerido para las funciones propias del usuario, a través del mecanismo que establezca el Departamento de Tecnologías de la Información.
PS-US-018	Es responsabilidad del usuario el contenido de los datos que circule en la red ya sea que los genere o solicite.
PS-US-019	El usuario externo que solicite acceso a la red de datos deberá cumplir con las políticas y lineamientos establecidos por el Departamento de Tecnologías de la Información.
PS-US-020	El Usuario quien tenga bajo su resguardo equipo de cómputo arrendado, será quien debe solicitar la reubicación y/o el cambio de resguardatario del equipo de cómputo, informando al Departamento de Tecnologías de la Información y al Centro de Atención a Usuarios de la empresa arrendadora, con la finalidad de mantener el inventario y resguardo actualizado.
PS-US-021	Es responsabilidad del usuario reportar errores de hardware y software, así como fallas en dispositivos de respaldo de energía presentados en equipos de arrendamiento, para que puedan ser canalizados con la empresa asignada para su atención, apegándose a sus procesos y tiempos de atención.

PS-US-022	Los titulares de las unidades administrativas deberán informar al Departamento de Tecnologías de la Información sobre algún cambio, innovación, acuerdo y/o mantenimiento sobre infraestructura tecnológica que se tenga contemplado para su evaluación y visto bueno.

POLÍTICAS DEL PERSONAL TÉCNICO CON FUNCIÓN INFORMÁTICA

PS-PT-001	Deberá contar preferentemente con un sitio alterno de respaldo, con la finalidad de proporcionar los elementos tecnológicos para asegurar la continuidad de la operación ante desastres naturales o incidentes de seguridad.
PS-PT-002	Es el autorizado para realizar la instalación, desinstalación, configuración del Software y Hardware del equipo de cómputo propiedad de la Secretaria en caso de equipo arrendado solo en caso de Software.
PS-PT-003	En lo referente a la seguridad de la red de datos, tendrá las siguientes funciones • Arquitectura, instalación, mantenimiento y gestión de la infraestructura activa de la red (switches, routers, etc.). • Mantenimiento, control y gestión de incidencias en la red. • Asignación de cuentas de usuario y contraseñas seguras para acceso a los recursos de la Red.
PS-PT-004	Generar y administrar las cuentas de usuario para acceso a los servicios de red, sistema operativo, aplicaciones web y bases de datos.
PS-PT-005	Deberá dar a conocer los lineamientos de atención de soporte técnico con las unidades administrativas usuarias, con la finalidad de garantizar el cumplimiento del servicio solicitado.
PS-PT-006	Verificar que todos los equipos y servidores utilizados en la operación, tengan instalado y actualizado un software antivirus.
PS-PT-007	Integrar carpetas con los diagramas, detalle de la infraestructura y configuraciones de la red.
PS-PT-008	Los componentes inalámbricos que forman parte de la red deben estar identificados y protegidos contra acceso lógico no autorizado.
PS-PT-009	Respaldar la información contenida en los servidores de datos, resguardarlos e identificarlos en medios de almacenamiento externo.
PS-PT-010	Responsable de cifrar la información de las bases de datos a respaldar en los sitios alternos.
PS-PT-011	Configurar el nivel de acceso de los usuarios a los servicios de red, sistemas web, bases de datos, entre otras, conforme a la autorización del Titular de la Unidad Administrativa.

PS-PT-012	Informar a Titular del Departamento de Tecnologías de la Información, cuando un servidor público con cuenta de correo electrónico Institucional deje de laborar en la Secretaría.
PS-PT-013	Actualizar los Sitios Web de responsabilidad en el Portal de la Secretaría, conforme a los estándares establecidos, por la Agencia Digital del Estado de México.
PS-PT-014	Tramitar ante la Agencia Digital del Estado de México a través del Departamento de Tecnologías de la Información, a efecto de validar y gestionar ante la instancia normativa: • El dictamen técnico para la adquisición, arrendamiento y/o contratación de bienes y servicios en materia de tecnologías de la información. • El formato de verificación de recepción para la validación técnica del equipo nuevo. • La autorización para envío al proveedor externo. • La opinión técnica para la baja de equipo. • La consultoría Técnica previa contratación de servicios informáticos. • Correo Electrónico Institucional. • Integración de trámites y servicios a la ventanilla electrónica única.
PS-PT-015	En caso de asignación de equipo arrendado a un nuevo usuario y sea requerida la reubicación, deberá reportarse en el Departamento de Tecnologías de la Información para que puedan ser canalizados con la empresa asignada y el técnico de esta empresa asista al lugar para realizar el cambio de resguardo y traslado del equipo de cómputo.
PS-PT-016	Deberá reportar a la mesa de servicio del equipo arrendado, los datos del ordenador en caso de detección de mal funcionamiento en hardware y software o para su reubicación.

POLÍTICAS DE SISTEMAS DE INFORMACIÓN

PS-SI-001	Es propiedad de la Secretaría, toda información institucional que se suministre, administre o sea generada, aún y cuando resida en equipos externos.
PS-SI-002	En el caso de que se realice la contratación de terceros para el desarrollo de sistemas, los derechos de uso, explotación y propiedad de los entregables o información generados serán a favor de la Secretaría, por lo que se deberán incluir cláusulas en los contratos establecidos.
PS-SI-003	Al término de los servicios contratados a terceros, se debe documentar y hacer constar por escrito por parte del proveedor que se compromete a entregar y/o devolver toda la información proporcionada o que se haya generado durante la prestación del servicio, así como el procedimiento y evidencia de la eliminación de información.
PS-SI-004	Se deberá controlar, resguardar y asegurar el código fuente, librerías, reportes y demás información que forme parte del diseño y desarrollo de las aplicaciones o sistemas.

PS-SI-005	Implementar mecanismos de control de usuarios por medio de niveles de acceso a la información, conforme a los criterios, requisitos y roles establecidos por la unidad administrativa usuaria.
PS-SI-006	Todo cambio (por adición o modificación de programas, pantallas y reportes) que afecte los sistemas de información y aplicaciones, debe ser solicitado por los usuarios responsables y a través de los canales oficiales.
PS-SI-007	Cada versión de un sistema de información generada deberá: • Tener un identificador único de la versión y la fecha de su realización visibles en la pantalla principal. • Ser respaldada en un repositorio permanente para su recuperación. • Contar con los manuales y documentación correspondientes actualizados.

DISPOSICIONES GENERALES:

- El desconocimiento de las presentes políticas no exime de su cumplimiento.
- La revisión de estas políticas debe realizarse al menos una vez al año y tomar en cuenta los resultados de las revisiones y auditorías para su actualización.

IMPREVISTOS:

- Los puntos no considerados en las presentes políticas que afecten la Seguridad y Control en materia de Tecnologías de la Información serán atendidos o resueltos por la instancia correspondiente.

Elaboró

Ing. Jocelyn Martínez Aviña
Líder A de Proyecto
Adscrita al Departamento de Tecnologías de la Información

Revisó

Ing. Luis Eduardo Aguilar Aguilar
Titular del Departamento de Tecnologías de la Información