Propósito

El presente documento, tiene como finalidad dar a conocer las Políticas y Estándares de Seguridad Informática que deberán observar las y los Servidores Públicos usuarios de los servicios de tecnologías de la información, para proteger adecuadamente los activos tecnológicos y la información correspondiente a la Subsecretaria de Tesorería en el ámbito de su competencia.

Introducción

La base para una operación confiable dentro de cualquier Organización, en materia de Seguridad Informática, comienza con la definición de políticas y estándares adecuados.
La Seguridad Informática, es la función en la cual se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la Subsecretaria de Tesorería en materia de seguridad.
Este documento se encuentra estructurado en cinco políticas generales de seguridad para las y los usuarios de los medios informáticos, así como de sus respectivos estándares que consideran los siguientes puntos:

- Seguridad de Personal
- Seguridad Física y Ambiental
- Administración de Operaciones de Cómputo
- Controles de Acceso Lógico.
- Cumplimiento

Objetivo

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal que se encuentre adscrito a la Subsecretaria de Tesorería, y con ello hacer de su conocimiento y para su cumplimiento dichos lineamientos, a fin de aumentar la eficiencia y eficacia de los recursos informáticos utilizados y asignados para el desempeño de sus funciones diarias.

Alcance

Aplica de manera obligatoria a las y los Servidores Públicos adscritos a la Subsecretaría de Tesorería, que fungen como usuarios del equipo de cómputo, sistemas internos, aplicaciones y servicios informáticos durante el cumplimiento de sus tareas. Siendo el documento que define las Políticas y Estándares de Seguridad.

DEFINICIONES

Código Malicioso:
Son los virus, malware o spyware que pueden encontrarse en el Equipo Informático.

Malware:
Programa malicioso, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el conocimiento de su propietario.

Spyware:
Programa espía, que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento del propietario del ordenador.

Error:
Acción involuntaria de los usuarios en el Equipo Informático y/o Programas.

Equipo Informático:
Conjunto de hardware (C.P.U, monitor, mouse, bocinas etc.)

Dolo:
Acción voluntaria del usuario, con la intención de llegar a los resultados obtenidos, los cuales son contra el Equipo Informático, software e información.

Fuga de Información:
Toda información confidencial, personal, reservada a la cual tengan acceso los usuarios y que por sí o por interpósita persona con o sin intención, ponga a disposición de persona no autorizada, ajena con o sin interés, causando un daño inminente a la Subsecretaría.

Herramientas Informáticas:
Son programas, aplicaciones o simplemente instrucciones usadas para efectuar otras tareas de modo más sencillo, entre otras se considera los Hardware y Software.

Ley:
Es la Ley de Responsabilidades Administrativas del Estado de México.

Incidente de Seguridad Informática:
Acceso del usuario (en su modalidad de consumado o tentativa), uso, divulgación, modificación o destrucción no autorizada de información, impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información, realizado por sí o por interpósita persona.

Mal Uso:
Es la utilización inadecuada por los usuarios, ya sea por sí o por interpósita persona respecto de los equipos Informáticos y/o software por error, dolo o negligencia.

Mecanismos Institucionales:
Son aquellos procesos reglamentados, definidos por la Ley, norma, reglamento que se encuentren completas y actualizadas, los cuales abarcan todas las funciones ejecutivas, directivas y técnicas para su puesta en práctica.

Medio de Almacenamiento de Información Compartido:
Sistemas de almacenamiento de datos, alojamiento, sistema de almacenamiento masivo concentrado.

Negligencia:
Es la falta de cuidado o el descuido realizado por el usuario de forma directa o por interpósita persona, el cual implica un riesgo para sí mismo o para terceros y se produce por la omisión de las consecuencias previsibles y posibles de la propia acción del descuido que realiza éstos pueden realizar con el equipo informático.

Portal:
Sitio web interno, que ofrece a los usuarios de la Subsecretaría, de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados a la información principal que utiliza día a día el servidor público, incluye: enlaces webs, documentos, aplicaciones, etc.

Recursos Informáticos:
Todos aquellos componentes de Hardware y Software que son necesarios para el buen funcionamiento y la optimización del trabajo.

Riesgos Reales
Evento negativo para la Información, Equipo Informático de la Subsecretaría, causado por los factores internos y externos en la asignación de recursos de la tecnología utilizada.

Riesgos Potenciales:
Los equipos de cómputo están sujetos al riesgo de que ocurra alguna eventualidad que los dañe debido a que no existe una seguridad total y las medidas de seguridad no pueden asegurar al 100% la protección en contra de las vulnerabilidades, es imprescindible realizar periódicamente un análisis de riesgos, para identificar las consecuencia probables o los riesgos asociados con las vulnerabilidades, y así, lograr un manejo de riesgo tras la implementación y mantenimiento de controles que reduzcan los efectos de éste a un nivel aceptable.

SEI:
Sistema Estatal de Informática.

Sistema:
Sistema Integral de Tesorería

Subsecretaría:
Subsecretaría de Tesorería

S.O.S.
Sistema Optimizado de Soporte, utilizado para reportar las incidencias que tengan los usuarios de la Subsecretaría de Tesorería, es necesario reportarse a través de éste, para que sea atendida su incidencia

Unidad
Unidad de Informática de la Subsecretaría.

Unidades Administrativas:
Subsecretaría, Unidad de Apoyo Técnico Financiero, Delegación Administrativa, Unidad, Dirección General de Crédito, Dirección General de Tesorería y/o a la Caja General de Gobierno.

Usuario:
Todo servidor (a) público (a) adscrito a la Subsecretaría, que tenga asignado un Equipo Informático y/o cuenta con acceso a los Sistemas de ésta; es decir, que sea beneficiario de bienes y servicios.

POLÍTICAS Y ESTÁNDARES DE SEGURIDAD PERSONAL

Política
Todo usuario se compromete a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos que establece para tal efecto la Ley de Transparencia y acceso a la Información Pública del Estado de México y Municipios, y a la Ley de Protección de Datos Personales del Estado de México, así como el estricto apego al presente Manual.

Obligaciones del usuario
Es responsabilidad de los usuarios, dar cumplimiento a las políticas y estándares de Seguridad Informática del presente Manual.

Acuerdos de uso y confidencialidad
Todos los usuarios, deberán firmar el Acuerdo de Confidencialidad que será emitido por la Unidad, lo que los compromete a conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información, así como a cumplir con lo establecido en el Manual.

Entrenamiento en Seguridad Informática
Los usuarios de la Subsecretaria tienen la obligación de conocer y saber lo que reglamenta el Manual, el cual se encuentra disponible en la siguiente dirección:

http://portal.tesoreria.edomex.net/

Medidas Disciplinarias

Cuando la Subsecretaria, identifique el incumplimiento al presente Manual, remitirá:

1. Llamada de atención en caso de que la falta no sea grave.
2. Dar vista al SEI, para el caso de información, cuando la falta sea grave para que éste realice las investigaciones y acciones correspondientes.
3. El reporte o denuncia correspondiente ante el Órgano de Control Interno, cuando la integridad de la información se encuentre en eminente riesgo o peligro, para los efectos de su competencia y atribuciones, en términos de la Ley.

POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Prevenir y en caso de ser procedente, restringir el acceso no autorizado, daños e interferencia a las instalaciones e información que corresponde a la Subsecretaria a personas ajenas en el ámbito de su competencia, o informar a su superior jerárquico, quien deberá realizar las acciones necesarias para salvaguardar los equipos de cómputo y de comunicaciones, así como las bases de datos de información, con medidas de seguridad y controles de acceso apropiados.

Resguardo y protección de Información.

- El usuario deberá reportar de forma inmediata a la Unidad, cuando detecte que existan riesgos reales o potenciales para equipos informáticos.
- El usuario tiene la obligación de proteger los CD-ROM, DVD-ROM, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen, pero contengan información de cualquier tipo, o bien sea reservada o confidencial propias de la Subsecretaría.
- Es responsabilidad del usuario evitar en todo momento la fuga de información que se encuentre almacenada en los equipos informáticos que tengan asignados.

Controles de Acceso físico

- Los usuarios, por sí o por otros, no deben mover o reubicar los equipos informáticos, instalar o desinstalar dispositivos, ni retirar sellos de los mismos. En caso de requerir estos servicios, deberá levantar un S.O.S en el Portal.
- El equipo informático asignado al usuario deberá ser para uso exclusivo de las funciones que le fueron conferidas en razón del cargo que ostenta dentro de la Subsecretaría, o aquellas adicionales que le sean encomendadas de forma extra oficial.
- Sera responsabilidad del usuario el manejo de las herramientas informáticas que se utilizan en su equipo, así como los riegos que se generen por mal uso.

- Se debe evitar colocar cualquier tipo de objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.
- Se debe mantener el equipo en un entorno limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos. Si se llega a presentar la situación y ésta es ajena a la voluntad del usuario, éste deberá levantar un S.O.S para informar tal situación, solicitando la intervención de la Unidad.

Mantenimiento de equipo

- Únicamente el personal autorizado por la Subsecretaria podrá llevar a cabo los servicios y reparaciones del equipo informático, por lo que los usuarios deberán solicitar por medios de un S.O.S los servicios y permitir el acceso a sus equipos.

Pérdida o transferencia del equipo.

- El usuario que tenga bajo su resguardo algún Equipo Informático será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo con la normatividad vigente en los casos de robo, extravió o pérdida del mismo.
- El usuario deberá dar aviso de inmediato a la unidad administrativa que corresponde de la desaparición, robo o extravió del Equipo Informático o accesorios bajo su resguardo.

POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO.

Política

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura de la Subsecretaria; de igual forma, deberá proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida.

Los usuarios de la Subsecretaria que hagan uso de Equipo Informático deben conocer y aplicar las medidas para la prevención de Código Malicioso.

Los usuarios pueden solicitar asesoría al respecto, a la Unidad por medio de un SOS.

Uso de medios de almacenamiento.

- Toda solicitud para utilizar un medio de almacenamiento de información compartido deberá contar con la autorización expresa del jefe inmediato del usuario y del titular del área dueña de la información.
- Los usuarios de la Subsecretaria deben conservar los registros o información que se encuentre activa y aquella que ha sido clasificada como reservada o confidencial, en términos de la Ley de Transparencia y Acceso a la información Pública del Estado de México y demás criterios y procedimientos establecidos en la materia.
- Los usuarios que inserten cualquier dispositivo de almacenamiento en el equipo informático, desde el momento en que éste sea insertado o enlazado al Equipo Informático, serán monitoreados en toda actividad realizada, para prevenir la fuga de información; en el supuesto de ser detectadas acciones tendientes a realizar Fuga de Información, se iniciarán las medidas de seguridad, dando vista al Órgano de Control Interno.

Instalación de Software

- Los usuarios que requieran la instalación de Software que no sea propiedad de la Subsecretaria, deberá justificar su uso y solicitar su instalación a través de un oficio firmado por el titular del área correspondiente, indicando el Equipo Informático al cual se instalara dicho Software
- Se considerará una falta el que los usuarios instalen cualquier tipo de programa (Software) en sus Equipos Informáticos asignados o estaciones de trabajo, que no esté autorizado y que comprometan la seguridad de la información, lo anterior en términos de la Ley.

Identificación del Incidente.

- El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a la Unidad a través de un SOS de manera inmediata.
- Cuando exista la sospecha o el conocimiento de que la información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Unidades Administrativas, el usuario deberá notificarlo al jefe inmediato superior o titular de la Unidad Administrativa de su adscripción.
- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información, debe ser reportado a la Unidad Administrativa de su adscripción.

Uso del correo Electrónico

- El servicio de correo electrónico es un servicio de comunicación y se debe hacer el uso de él, acatando todas las disposiciones de seguridad diseñadas para la utilización y evitar el uso o introducción de software malicioso a la red institucional, en términos de la Ley de Gobierno Digital o cualquier otra homologa vigente.
- Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- La Subsecretaria, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado las Políticas y Estándares de Seguridad Informáticas o realizado acciones no autorizadas.
- Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de su funciones y atribuciones, a través del correo Instruccional que le proporcionó la Subsecretaria.
- El usuario deberá cuidar en todo momento la utilización de un lenguaje apropiado, evitando palabras ofensivas o altisonantes.
- Todo uso indebido del servicio de correo electrónico será motivo de suspensión temporal de la cuenta de correo o según sea necesario la eliminación total de la cuenta del sistema.

Controles contra código malicioso

- Para prevenir infecciones por virus informático, los usuarios deben evitar hacer uso de cualquier clase de Software que no haya sido instalado y validado por la Unidad.
- Los usuarios, deben verificar que la información y los medios de almacenamiento considerando al menos memorias USB y CD-ROM, estén libres cualquier tipo de virus, por lo cual deberán al momento de enlazar dichos medios, la ejecución sobre estos del Software Antivirus.
- El usuario debe verificar mediante el Software de Antivirus que se encuentren libres de virus todos los archivos de la computadora, base de datos, documentos etc., que sean proporcionados por personal tanto interno como externo.
- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Unidad, solicitando la revisión de este, para la detección y erradicación del virus.
- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Unidad, tales como:
    - ✓ Antivirus
    - ✓ Correo Electrónico

- ✓ Paquetería Office
- ✓ Navegadores
- ✓ O cualquier otro programa

- Debido a que algunos virus son extremadamente complejos, ningún usuario de la Subsecretaria debe intentar erradicarlos de las computadoras, la acción a realizar es mediante un reporte a la Unidad de Informática a la brevedad.

Permisos de uso de Internet

- El acceso a internet previsto a los usuarios es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
- La asignación del servicio de internet deberá solicitarse por escrito, señalando los motivos por los que se requiere el servicio; esta solicitud deberá hacerla el titular del área correspondiente.
- Todos los accesos a internet tienen que ser a través de los canales de acceso previstos por la Subsecretaria.
- Los usuarios con acceso a Internet deben reportar todos los incidentes de seguridad informática a la Unidad inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
- Los usuarios con servicio de Internet, al utilizar el servicio aceptan que:
  - ✓ Serán sujetos de monitoreo de las actividades que realicen en Internet.
  - ✓ Saben que existe la prohibición al acceso a paginas no autorizadas.
  - ✓ Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
  - ✓ Saben que existe la prohibición de descarga de software sin la autorización correspondiente.
  - ✓ La utilización de Internet es para desempeño de su función y puesto y no para propósitos personales.

- Los esquemas de permisos de acceso a Internet son:
  1. **Limitado**: Paginas de Gobierno Únicamente, bancos
  2. **Básico**: Limitado + Internet General (paginas seguras, Educación, Salud, Noticias, etc.)
  3. **Intermedio**: Básico + Internet General sin Redes Sociales
  4. **Avanzado:** Intermedio + Redes Sociales

POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información tecnológica de la Subsecretaria, por lo cual deberá mantenerlo de forma confidencial.

Controles de Acceso Lógico

- Está prohibido que los usuarios utilicen la información tecnológica de la Subsecretaria para obtener acceso no autorizado a la información u otros sistemas de información.
- Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que reciben para el uso y acceso a los recursos.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones y aplicaciones tecnológicas de la Subsecretaria, a menos que se tenga autorización.
- Cada usuario que accede a la infraestructura tecnológica debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuarios por varios usuarios.
- El usuario tiene prohibido compartir su identificador de usuarios y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezca, salvo que pruebe que le fueron usurpados esos controles, de igual forma tiene prohibido usar el identificador de usuarios y contraseñas de otros. En términos del Acuerdo de Confidencialidad.

Administración de privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios

Equipo desatendido

Los usuarios deberán mantener sus Equipos Informáticos con controles de acceso como contraseñas y protectores de pantalla, como una medida de seguridad cuando el usuario necesite ausentarse de su espacio de trabajo por un tiempo indefinido.

Administración y uso de contraseñas

- La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas será realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

- Cuando un usuario olvide, bloquee o extravié su contraseña, deberá reportarlo mediante un SOS, para que se realicen las acciones correspondientes y se le pueda reestablecer la contraseña.
- Está prohibido que los identificadores de usuarios y contraseña se encuentren visibles en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.
- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente.
- Los cambios o desbloqueos de contraseñas deberán ser solicitados por medios de un SOS.

POLÍTICAS Y CUMPLIMIENTOS DE SEGURIDAD INFORMÁTICA

Política

La Subsecretaria, tiene como una de sus funciones la de proponer y revisar el cumplimiento de las normas y políticas de seguridad informática, que garanticen acciones preventivas y correctivas para salvaguardar los Equipos Informáticos y sus instalaciones, comunicaciones y bases de datos de información, así como planear el desarrollo tecnológico al interior de la Subsecretaria.

Derechos de propiedad Intelectual

- Está prohibido realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Subsecretaria.
- Los sistemas desarrollados por personal, interno o externo, para uso exclusivo de sistemas o proyectos, son propiedad de la Subsecretaria.

Revisión del cumplimiento

- La Subsecretaria, realizará acciones de verificación del cumplimiento del Manual para usuarios.
- La Subsecretaria, podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar las actividades de proceso que ejecuta y la estructura de archivos que se procesan.

Violaciones de seguridad informática

- Está prohibido el uso de herramientas de Hardware o Software para violar los controles de seguridad informática.
- Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnologías de la Información.

- Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación correspondiente por la unidad administrativa
- Ningún usuario debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos de que estas pruebas sean controladas y aprobadas. Por la unidad administrativa
- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o introducir cualquier tipo de código o programa (código malicioso) diseñado para dañar o afectar el desempeño, acceso las computadoras y sistemas, o para obtener información de la Subsecretaria.

INCUMPLIMIENTO

Cualquier incumplimiento por parte de los Usuarios, por sí o por interpósita persona, dará lugar a las medidas de seguridad referidas en el presente Manual, en términos de lo dispuesto por la Ley de Responsabilidades Administrativas del Estado de México, Ley de Transparencia y Acceso a la Información Pública, Ley de Protección de Datos Personales, Ley de Gobierno Digital, y toda aquella normatividad aplicable para tal efecto.