EPMT-SD
Empresa Pública Municipal
Transporte Terrestre y Tránsito

POLÍTICAS DE SEGURIDAD INFORMÁTICA

Subdirección de Informática y Redes

2025

Tabla de contenido

Propósito.

El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la EPMT-SD.

Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la EPMT-SD en materia de seguridad.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con 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 de la EPMT-SD, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

Alcance

El documento define las Políticas y Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos de la EPMT-SD.

Justificación

La Subdirección de Informática y Redes de la EPMT-SD está facultada para definir Políticas y Estándares en materia informática.

Sanciones por Incumplimiento

El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Beneficios

Las Políticas y Estándares de Seguridad Informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos e información de la EPMT-SD.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política.

Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de la EPMT-SD, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para usuarios.

1.1 .Obligaciones De los Usuarios.

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

1.2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información de la EPMT-SD.

1.3. Entrenamiento en Seguridad Informática.

Todo funcionario de la EPMT-SD deberá:

Conocer y aplicar el Manual de Políticas y Estándares de Seguridad Informática para Usuarios de la EPMT-SD, ya que el desconocimiento de las políticas que se detallarán en el presente documento no exime de culpa en caso de incumplimiento.

1.4. Medidas Disciplinarias

Cuando la Subdirección de Informática y Redes detecte el incumplimiento al presente Manual remitirá el reporte o denuncia correspondiente al Órgano Interno de Control de la EPMT-SD, para los efectos de su competencia y atribuciones.

2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la EPMT-SD, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y los diferentes Centros de atención de la EPMT-SD.

2.1 Resguardo y protección de la información.

El usuario deberá reportar de forma inmediata a la Subdirección de Informática y Redes, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad del usuario evitar en todo momento la fuga de la información de la EPMT-SD, que se encuentre almacenada en los equipos de cómputo personal a su cargo.

2.2. Controles de acceso físico

Prohibir que personal ajeno a su adscripción, intente cambiar un periférico del equipo de computo a su cargo, para esto es necesario que cada usuario tenga a la mano el listado de los equipos asignados a su cargo, para su inmediata verificación

En caso de detectar cualquier anomalía deberá reportar inmediatamente a la Subdirección Administrativa y Talento Humano

2.3. Seguridad en áreas de trabajo

El cuarto de equipos de la Subdirección de Informática y Redes de la EPMT-SD, es una área restringida, por lo que sólo el personal autorizado por la Subdirección de Informática y Redes puede acceder a ellos.

Así mismo, cada usuario debe cuidar el uso del o los equipos informáticos bajo su custodio.

2.4. Protección y ubicación de los equipos

2.4.1. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Subdirección de Informática y Redes.

2.4.2. Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.4.3. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

2.4.4. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso.

2.4.5. Evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

2.4.6. Mantener el equipo informático en un entorno limpio y sin humedad.

2.4.7. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

2.4.8. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Subdirección de Informática y Redes a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.4.9. La manipulación de los equipos informáticos solo debe ser realizado por el personal de la Subdirección de Informática y Redes, ante cualquier evento

2.5. Mantenimiento de equipo

2.5.1. Únicamente el personal autorizado por la Subdirección de Informática y Redes podrá llevar a cabo los servicios de Mantenimiento preventivo y reparaciones a los equipos informáticos.

2.5.2. Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal de la Subdirección de Informática y Redes

2.6. Pérdida o transferencia de equipo

2.6.1. El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.6.2. Ante el ausentismo mayor a 3 dias por parte del usuario, por cualquiera que fuese el motivo, el resguardo para los equipos informáticos a su cargo deberá transferirse la custodia de los mismos a su reemplazo o su jefe inmediato, debiendo hacer constar en acta de entrega recepción la custodia de estos e informar por escrito a la Subdirección Administrativa y Talento Humano para el respectivo control de bienes

2.6.3. El usuario deberá dar aviso de inmediato a la Subdirección Administrativa y Talento Humano por la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7. Uso de dispositivos especiales

2.7.1. El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen.

2.7.2. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le brinde.

2.8. Daño del equipo.

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo así

mismo el accesorio afectado. Para tal caso se determinará la causa de dicha descompostura.

3. 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 EPMT-SD. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la EPMT-SD o hacia redes externas como internet.

Los usuarios de la EPMT-SD que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir a la Subdirección de Informática y Redes, para solicitar asesoría.

3.1. Uso de medios de almacenamiento

3.1.1. Toda solicitud para utilizar un medio de almacenamiento de información compartido, deberá contar con la autorización del jefe inmediato del usuario y del titular del área dueña de la información.

Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con sello y firma a la Subdirección de Informática y Redes.

3.1.2. Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la Subdirección de Informática y Redes.

3.1.3. Los respaldos de la información relacionada con la EPMT-SD, que haya sido almacenada en cualquier medio o dispositivo magnético, debe ser cuidada sigilosamente y será de responsabilidad del usuario el manejo de la misma

3.1.4. Las actividades que realicen los usuarios de la EPMT-SD en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

3.2. Instalación de Software

3.2.1. Está prohibido que los usuarios instalen software que no sea propiedad de la EPMT-SD y que sean ajenos a la competencia de su actividades cotidianas, en caso de detectarse esto, la Subdirección de Informática y Redes tiene la facultad de desinstalar inmediatamente estos software no autorizados.

De requerir este tipo de software, se deberá justificar plenamente por escrito detallando el equipo de cómputo en el que se instalará y el uso de este, en cuyo documento deberá tener la aprobación de su inmediato superior

3.3. Identificación del incidente

3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a la Subdirección de Informática y Redes o al representante de ésta en su zona, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2.Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Subdirecciónes administrativas competentes, el usuario informático deberá notificar al titular de su adscripción.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la EPMT-SD, debe ser reportado a la Subdirección de Informática y Redes.

3.4. Administración de la configuración

Los usuarios de las áreas de la EPMT-SD, no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la EPMT-SD, sin la debida autorización por escrito por parte de la Subdirección de Informática y Redes.

3.5. Seguridad de la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Subdirección de Informática y Redes en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la EPMT-SD, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

3.6. Uso del correo electrónico.

3.6.1. Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno o en lo posible a su reemplazo, quedando prohibido hacerlo a una dirección de correo electrónico externa a la EPMT-SD, a menos que cuente con la autorización del titular del área de adscripción.

3.6.2. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la EPMT-SD. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3. Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la Subdirección de Informática y Redes.

3.6.4. La EPMT-SD, 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 violando políticas de Seguridad Informática de la EPMT-SD o realizado acciones no autorizadas.

Como la información del correo electrónico institucional de la EPMT-SD es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

3.6.5. El usuario debe de utilizar el correo electrónico de la EPMT-SD, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

3.6.6. La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito a la Subdirección de Informática y Redes, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del jefe inmediato del área que corresponda.

3.6.7. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.7. Controles contra código malicioso.

3.7.1. Para prevenir infecciones por virus informáticos, los usuarios de la EPMT-SD, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Subdirección de Informática y Redes.

3.7.2. Los usuarios de la EPMT-SD, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, discos flexibles, CD´s, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Subdirección de Informática y Redes.

3.7.3. El usuario debe verificar mediante el software de antivirus autorizado por la Subdirección de Informática y Redes que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

3.7.4. Ningún usuario de la EPMT-SD debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ambientes o plataformas de la EPMT-SD. El incumplimiento de este estándar será considerado una falta grave.

3.7.5. Ningún usuario ni empleado de la EPMT-SD o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de Subdirección de Informática y Redes.

3.7.6. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Subdirección de Informática y Redes para la detección y erradicación del virus.

3.7.7. Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica a la Subdirección de Informática y Redes. las actualizaciones del software de antivirus.

3.7.8. 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 Subdirección de Informática y Redes en programas tales como:

- Antivirus;
- Correo electrónico;
- Paquetería Office;
- Navegadores; u
- Otros programas.

3.7.9. Debido a que algunos virus son extremadamente complejos, ningún usuario de la EPMT-SD debe intentar erradicarlos de las computadoras, lo indicado es llamar al personal de la Subdirección de Informática y Redes para que sean ellos quienes lo solucionen.

3.8. Permisos de uso de Internet

3.8.1. El acceso a internet provisto a los usuarios de la EPMT-SD es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el Órgano Interno de la EPMT-SD.

3.8.2. La asignación del servicio de internet, deberá solicitarse por escrito a la Subdirección de Informática y Redes, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del jefe inmediato.

3.8.3. Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por EPMT-SD.

3.8.3. Los usuarios con acceso a Internet de la EPMT-SD tienen que reportar todos los incidentes de seguridad informática, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.4. El acceso y uso de dispositivos externos para la conexión a internet de los equipos de cómputo de propiedad de la EPMT-SD, debe ser previamente autorizado por la Subdirección de Informática y Redes.

3.8.5. Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas 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 de la Subdirección de Informática y Redes.
- La utilización de internet es para el desempeño de su función y puesto en la EPMT-SD y no para propósitos personales.

3.8.6. Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

NIVEL 1: Sin restricciones: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

NIVEL 2: Intermedio: Los usuarios podrán hacer uso de internet, acceso a correo electrónico externo y páginas gubernamentales, aplicándose las políticas de seguridad y navegación.

NIVEL 3: Internet restringido: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación

4. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Política.

Cada usuario es responsable del acceso que le sea proporcionado; esto es, de su identificador de usuario (userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica de la EPMT-SD, por lo cual deberá mantenerlo de forma confidencial.

La Subdirección de Informática y Redes, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica de la EPMT-SD, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones.

4.1. Controles de acceso lógico

4.1.1. El acceso a la infraestructura tecnológica de la EPMT-SD para el personal externo debe ser autorizado por la Subdirección de Informática y Redes, previa solicitud por escrito del o los interesados.

4.1.2. Está prohibido que los usuarios utilicen la infraestructura tecnológica de la EPMT-SD para obtener acceso no autorizado a la información u otros sistemas de información de la EPMT-SD.

4.1.3. Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.4. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Subdirección de Informática y Redes antes de poder usar la infraestructura tecnológica de la EPMT-SD.

4.1.5. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la EPMT-SD, a menos que se tenga autorización de la Subdirección de Informática y Redes.

4.1.6. Cada usuario que accede a la infraestructura tecnológica de la EPMT-SD debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

4.1.7. Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

4.1.8. Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

4.2. Administración de privilegios

4.2.1. Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la EPMT-SD, deberán ser notificados por escrito o vía correo electrónico a la Subdirección de Informática y Redes, con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.3. Equipo desatendido

4.3.1 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por la Subdirección de Informática y Redes, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

4.4. Administración y uso de contraseñas

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

4.4.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito a la Subdirección de Informática y Redes, indicando si es de acceso a la red o a módulos de sistemas implementados por la Subdirección de Informática y Redes para que se le proporcione una nueva contraseña.

4.4.3. La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la Subdirección de Informática y Redes como empleado de la EPMT-SD.

4.4.4. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible 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.

4.4.5. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10).Estos caracteres deben ser alfanuméricos, o sea, números y letras;
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario; y Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.4.7. La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

4.4.8. Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.

4.4.9. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

4.4.10. Los cambios o desbloqueo de contraseñas solicitados por el usuario a la Subdirección de Informática y Redes serán solicitados mediante oficio sellado y firmado por el jefe inmediato del usuario que lo requiere.

4.4.11. Todo usuario deberá actualizar sus contraseñas por los menos 2 veces al año.

4.5. Control de accesos remotos

4.5.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la Subdirección de Informática y Redes.

4.5.2. La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la Subdirección de Informática y Redes.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política

La Subdirección de Informática y Redes., es la encargada de fijar las bases de la política informática que permitan conocer y planear el desarrollo tecnológico al interior de la EPMT-SD"

5.1. Derechos de Propiedad Intelectual.

5.1.1. Está prohibido por las leyes de derechos de autor y por la EPMT-SD, realizar copia no autorizada de software, ya sea adquirido o desarrollado por la EPMT-SD.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte de la Subdirección de Informática y Redes, o sea coordinado por ésta, son propiedad intelectual de la EPMT-SD.

5.2. Revisiones del cumplimiento.

5.2.1. La Subdirección de Informática y Redes realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.

5.2.2. La Subdirección de Informática y Redes podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

5.3. Violaciones de seguridad informática

5.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la Subdirección de Informática y Redes.

5.3.2. Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información.

Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación de la Subdirección de Informática y Redes, con excepción de los Órganos Fiscalizadores.

5.3.3. Ningún usuario de la EPMT-SD debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Subdirección de Informática y Redes.

5.3.4. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para autoreplicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información de la EPMT-SD.

GLOSARIO

TÉRMINO	SIGNIFICADO
(A)	
Acceso	Es el privilegio de una persona para utilizar un objeto o infraestructura.
Acceso Físico	Es la actividad de ingresar a un área.
Acceso Lógico	Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.
Acceso Remoto	Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Antivirus	Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
Ataque	Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.
(B)	

Base de datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.
(C)	
Confidencialidad	Se refiere a la obligación de los servidores judiciales a no divulgar Información a personal no autorizado para su conocimiento.
Contraseña	Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema,
Control de Acceso	Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso
Copyright	Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite
(D)	
Disponibilidad	Se refiere a que la información esté disponible en el momento que se necesite.
(E)	
Estándar	Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.
(F)	
Falta administrativa	Acción u omisión contemplada por la normatividad aplicable a la actividad de un servidor, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.
FTP	Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
(G)	
Gusano	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.
(H)	
Hardware	Se refiere a las características técnicas y físicas de las computadoras.

Herramientas de seguridad	Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.
(I)	
Identificador de Usuario	Nombre de usuario (también referido como UserID) único asignado a un servidor judicial para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice.
Incidente de Seguridad	Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.
Integridad	Se refiere a la pérdida ó deficiencia en la autorización, totalidad ó exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.
Internet	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes (world wide web) en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.
Intrusión	Es la acción de introducirse o acceder sin autorización a un activo.
(M)	
Maltrato	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la EPMT-SD Se contemplan dentro de éste al descuido y la negligencia.
Malware	Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, *spyware*, *troyanos*, *rootkits*, *backdoors, adware* y gusanos.
Mecanismos de seguridad o de	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para
control	la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios de almacenamient	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD´s, DVD´s, etc.)
Módem	Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten
(N)	

"Necesidad de saber" principio	Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.
(P)	
Password	Véase Contraseña.
(R)	
Respaldo	Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.
(S)	
Subdirección de Informática y Redes	Se refiere a la Subdirección de Informática y Redes de la EPMT-SD.
Servidor	Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Sitio Web	El sitio web es un lugar virtual en el ambiente de internet, el cual
	proporciona información diversa para el interés del público, donde
Software	Programas y documentación de respaldo que permite y facilita el
Spyware	Código malicioso desarrollado para infiltrar a la información de un
(U)	
UserID	Véase Identificador de Usuario.
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).
(V)	

Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

Suscrito a los 12 días del mes de febrero de 2025.

Elaborado Por: Ing. Cristhian Daniel Santos **Especialista de Informática y Redes**	
Revisado Por : Ing. Polo Sánchez Jara **Subdirector de Informática y Redes**	
Autorizado Por : Dr. Héctor Fiallo Sandoval **Gerente General**	