COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

INSTITUTO MEXICANO DEL TRANSPORTE

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

VIGENCIA: Octubre 2024

N° DE REGISTRO: IMT-NIA-NSA-SM-0004

Tabla de contenido

I. INTRODUCCIÓN

En el ámbito de las Tecnologías de la Información y Comunicaciones (TIC), el Instituto Mexicano del Transporte (IMT) está comprometido a proteger a su personal, a los grupos de la sociedad que interactúan con él y a la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), de acciones ilegales o perjudiciales que se cometan en esta materia.

El IMT suministra a su personal los siguientes recursos de TIC: el Internet, la Intranet, el correo electrónico, los equipos de cómputo (hardware), los sistemas operativos y aplicativos (software), la telefonía y los medios de almacenamiento de información, por lo que deben ser utilizados con fines estrictamente laborales.

La elaboración, difusión e implementación de las Políticas de Seguridad de la Información es una responsabilidad de la División de Telemática, prevista en el Manual de Organización; a través de este documento se dan diversas disposiciones generales para el buen uso y cuidado de los bienes y servicios de TIC proporcionados a los servidores públicos que forman parte del IMT, colaboradores y visitantes del IMT.

II. FUNDAMENTO LEGAL

Leyes:

Ley Federal de Responsabilidades de los Servidores Públicos
D.O.F. 31-XII-1982, última reforma D.O.F. 01-IV-2024

Ley Federal de Derechos de Autor
D.O.F. 24-XII-1996, última reforma D.O.F. 01-VII-2020

Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público
D.O.F 04-I-2000, última reforma D.O.F. 25-V-2021

Ley Federal de Telecomunicaciones y Radiodifusión
D.O.F.14-VII-2014, última reforma D.O.F. 01-IV-2024

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
D.O.F.11-VI-2002, última reforma D.O.F. 08-VI-2012

Ley Federal de Protección de Datos Personales en Posesión de los Particulares
D.O.F.05- VII-2010

Reglamentos:

Reglamento Interior de la Secretaría de Infraestructura, Comunicaciones y Transportes D.O.F. 8-I-2009 actualizado 29-I-2024

Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público D.O.F. 20-VIII-2001, última reforma D.O.F 14-II-2024

Acuerdos:

Acuerdo por el que se emiten las Disposiciones en Materia de Control Interno D.O.F. 12-VII-2010, última reforma D.O.F. 05-IX-2018

Acuerdo por el que emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicaciones, y la seguridad de la información en la Administración Pública Federal. D.O.F. 08-V-2014, última reforma D.O.F. 06-IX-2021

ACUERDO por el que se emiten las Disposiciones y el Manual Administrativo de Aplicación General en Materia de Control Interno. D.O.F. 03/11/2016, última reforma D.O.F.05-IX-2018

Códigos:

Código Penal Federal D.O.F. 14-III-2014, última reforma 01-VII-2020, Artículo 211 bis1, 211 bis2, 211 bis3, 211 bis4, 211 bis5, 211 bis6

Documentos Normativo-Administrativos:

Estrategia Digital Nacional 2021-2024
DOF: 06/09/2021

Condiciones Generales de Trabajo de la Secretaría de Infraestructura, Comunicaciones y Transportes 2022/2024, firmada el 2-12-2021

Manual de Organización del IMT.
Agosto 2018

PROGRAMA Nacional de Combate a la Corrupción y a la Impunidad, y de Mejora de la Gestión Pública 2019-2024. DOF: 30-VIII-2019

Programa Sectorial de Comunicaciones y Transportes 2020-2024. DOF: 2-VII- 2020

III. DEFINICIONES

Para los efectos de estos lineamientos se entenderá por:

a) **Acceso:** permisos que permiten a los usuarios ingresar a un área física o aplicación informática.

b) **Administrador de sistema:** es la persona encargada de gestionar, configurar, monitorear y dar mantenimiento a un sistema en producción.

c) **Antivirus:** aplicación diseñada para detectar, bloquear y, en su caso, eliminar virus informático, preferentemente antes de que cause daños a un bien telemático.

d) **Autenticación:** método para acreditar al usuario autorizado.

e) **Bienes de TIC:** equipo de cómputo, software, periféricos, infraestructura y servicios que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

f) **Bitácora electrónica:** es una aplicación en donde se registran cronológicamente los eventos e incidentes que les ocurren a los sistemas de información y/o a las plataformas sobre las que operan.

g) **Borrado seguro de información:** es el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable, la información contenida en medios de almacenamiento digital.

h) **Buzón de voz:** sistema centralizado que permite al usuario recibir, almacenar y gestionar mensajes de voz de las personas que le llaman, cuando se encuentra ausente o con la línea ocupada.

i) **Centro de Datos:** es el espacio físico donde se concentran los recursos necesarios para el procesamiento de la información de una Institución o proveedor de servicios, consistente en equipo informático y redes de comunicaciones.

j) **Cert-MX:** Centro Especializado en Respuesta Tecnológica, de México.

k) Código malicioso: programación malintencionada, incluida deliberadamente en mensajes de correo electrónico, documentos o páginas web, que ocasiona alguna función no deseada en los equipos de cómputo.

l) Confidencialidad: garantizar que la información esté disponible solamente para las personas y procesos autorizados. La información confidencial será protegida para que no sea divulgada, comunicada, reproducida o revelada a terceras personas.

m) Conservación de la información crítica: asegurar la preservación, mediante el establecimiento de políticas y procedimientos de respaldo y recuperación en medios y dispositivos específicos.

n) Contraseña: serie de caracteres alfanuméricos, que complementa a la cuenta de acceso y que permite al usuario ingresar a un sistema de información.

o) Credenciales: información utilizada para autenticar al usuario, como el nombre de usuario, contraseña, token de acceso o certificado digital.

p) Datos: es un valor o referente que recibe la computadora, que puede ser procesado, almacenado y convertido en información útil.

q) Desarrollo de software: es el diseño, implementación, pruebas y puesta a punto de un sistema informático.

r) Disponibilidad de información: asegurar que sólo los usuarios autorizados tengan acceso a determinada información, en el momento que la requieran.

s) Escaneo de puertos: verificación de puertos TCP/UPD abiertos en un equipo de cómputo.

t) FTP (**Protocolo de Transferencia de Archivos)**: es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red, basado en la arquitectura cliente-servidor.

u) Identificación: proceso mediante el cual un sistema reconoce a un usuario o dispositivo, antes de permitirle acceso a recursos específicos.

v) IDFs (Instalación de Distribución Intermedia o Intermediate Distribution Frame por sus siglas en inglés**):** sitios de comunicación secundaria, que son uniones críticas en la infraestructura de una red; cumplen distintas funciones dentro de la arquitectura de conectividad de una organización.

w) Incidente de seguridad: es un evento no deseado o inesperado, que atenta contra la confidencialidad, integridad y disponibilidad de la información, así como a los bienes de TIC de la institución, incluido el acceso no autorizado o no programado a éstos.

x) Información: conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o del sistema que lo recibe.

y) Integridad: garantizar que la información puede ser generada, modificada y eliminada sólo por personal autorizado, asegurando que la información almacenada o circulante no pueda ser corrompida ni alterada intencional o accidentalmente.

z) Licencia de software: permiso legal otorgado por un tercero con facultades para ello, para utilizar un producto.

aa) MDF (Instalación Principal de Distribución o Main Distribution Frame, por sus siglas en inglés**):** sitios de comunicación primaria donde se reciben los servicios de Internet, Internet 2, Intranet SICT y Telefonía, para después distribuirlos a los IDF's del Instituto.

bb) Permisos: autorizaciones necesarias para realizar ciertas actividades, o acceder a recursos específicos dentro de un sistema o red.

cc) Pruebas de vulnerabilidad: consisten en identificar las brechas de seguridad de la información que se pueden presentar en los bienes de TIC.

dd) Red social: es un sistema que involucra a un conjunto de personas, que tienen intereses comunes, y que se organizan para intercambiar información y potenciar sus recursos, en forma dinámica.

ee) Respaldo de la información: resguardo de los datos más relevantes, que se generen en el IMT, utilizando un almacenamiento dedicado.

ff) Seguridad de la Información: es la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

gg) Sistema de información: conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para cubrir una necesidad o un objetivo.

hh) Sitio restringido de TIC: área sensible que resguarda bienes de TIC, en donde solo pueden acceder las personas autorizadas.

ii) Software: conjunto de componentes o instrucciones lógicas, para la automatización de funciones específicas.

jj) Virus: programa de cómputo que tiene como objetivo causar una alteración en un bien telemático, comprometiendo la seguridad de la información.

IV. OBJETIVO

Establecer el marco de actuación que deben seguir los servidores públicos que forman parte del IMT, colaboradores (tesistas o personal contratado por honorarios) y visitantes del IMT respecto al buen uso y aprovechamiento de los bienes y servicios de TIC, para asegurar la integridad de la información.

V. ÁMBITO DE APLICACIÓN

Es responsabilidad de todos los servidores públicos que forman parte del IMT, colaboradores y visitantes conocer y cumplir las presentes Políticas de Seguridad de la Información del Instituto Mexicano del Transporte, así como los procedimientos y guías que de ellas emanen, conduciendo sus actividades en ese sentido.

Las presentes Políticas de Seguridad de la Información del Instituto Mexicano del Transporte aplican a todos los servidores públicos que forman parte del IMT, personal que realice estancias de investigación y todos aquellos prestadores o proveedores de

bienes o servicios, consultores o demás grupos de la sociedad que interactúan con el Instituto, cuando tengan acceso o hagan uso de la información o de los bienes de TIC.

Los responsables de hacer cumplir las Políticas de la Información del Instituto Mexicano del Transporte son: el Director General, los Coordinadores de las Áreas, los Jefes de División y los Jefes de Unidad.

VII. ACCIONES ADMINISTRATIVAS Y LEGALES EN CASOS DE INCUMPLIMIENTO

Para los casos en los que los servidores públicos que forman parte del IMT, colaboradores y visitantes, incumplan con lo definido en estas Políticas de Seguridad de la Información, son las siguientes:

Tratándose de servidores públicos que forman parte del IMT:

a) De acuerdo con la gravedad, la Dirección General notificará severo extrañamiento al servidor público infractor; el cual se anexará a su expediente personal.

b) De reincidir, o de acuerdo con la gravedad, se dará vista al Área de Especialidad en Responsabilidades en el Ramo de Infraestructura, Comunicaciones y Transportes del Órgano de Control y Fiscalización, para que proceda con la sanción correspondiente.

c) De así considerarlo, se dará vista al área especializada de la Fiscalía General, para que proceda con la sanción correspondiente.

Tratándose de colaboradores y visitantes:

a) De comprobarse la vulneración a la seguridad de la información, se dará vista al área especializada de la Fiscalía General, para que proceda con la sanción correspondiente.

VIII. DISPOSICIONES GENERALES

El propósito fundamental de estas políticas es establecer el marco de actuación sobre el aprovechamiento de los bienes y servicios de TIC, para mantener la seguridad de la información con que cuenta este Instituto, así como tomar medidas colectivas eficaces

para prevenir ataques, eliminar amenazas, y suprimir actos de agresión u otros quebrantamientos.

Sección 1. Política de Correo Electrónico Institucional

Objetivo

Establecer las políticas acciones del uso apropiado del Correo Electrónico que proporciona el IMT a sus empleados, considerando: la gestión, operación y medidas de seguridad necesarias para garantizar la continuidad de este servicio.

Ámbito de aplicación

Aplica a todos los servidores públicos que forman parte del IMT que dispongan de una cuenta de correo electrónico institucional.

Política

1. El uso del servicio de correo electrónico institucional será proporcionado sólo a empleados, para fines estrictamente laborales.

2. Dado que el servicio de correo electrónico hace uso de los recursos del Instituto, los mensajes podrán ser monitoreados con fines de auditoría.

3. El envío de archivos adjuntos está autorizado siempre que la clasificación de la información así lo permita, y que el tamaño total de archivos anexos no exceda los 10MB.

4. El tamaño asignado de buzón en el servidor de correo será de 128 MB para personal operativo y 512 MB para los Jefes de Área y sus secretarias. En casos extraordinarios (comisiones, licencias médicas o vacaciones) la capacidad del buzón se podrá ampliar, mediante una solicitud por correo electrónico al Responsable del servicio de correo electrónico.

5. El titular de la cuenta de correo electrónico es el responsable de mantener la confidencialidad de su contraseña, así como de los mensajes y el contenido que en ellos genere.

6. Las contraseñas se actualizarán periódicamente, de acuerdo con la Política para Contraseñas.

7. Todos los correos electrónicos entrantes deben ser tratados con extremo cuidado, debido al riesgo inherente a la seguridad de la información: antes de abrir cualquier correo electrónico, los usuarios deberán verificar primero que la cuenta

del remitente sea válida, que el sujeto y que los contextos de la conversación sean coherentes.

8. Antes de abrir un archivo adjunto o hipervínculo, verificar su autenticidad.

9. Los correos recibidos de remitentes desconocidos deben ser borrados permanentemente sin ser abiertos.

10. Todo usuario con una cuenta institucional asignada debe tratar la información que genere como propiedad del Instituto.

11. No se podrán usar cuentas de correo ajenas al IMT para el envío de documentos o información relativa a las funciones adscritas a su cargo.

12. Será considerado como malintencionado suplantar la identidad de un usuario de correo electrónico.

Sección 2. Política de los Sistemas de Información

Objetivo

Garantizar el uso adecuado y eficiente de los sistemas informáticos del Instituto Mexicano del Transporte, mediante la implementación de acciones alineadas con las normativas institucionales, que promueven un acceso controlado y responsable a los recursos tecnológicos, con el fin de proteger la información confidencial y asegurar la continuidad de las actividades operativas.

Ámbito de aplicación

Aplica a todos los servidores públicos que forman parte del IMT que accedan a cualquier sistema de información institucional.

Política

1. La titularidad de los sistemas informáticos desarrollados en el IMT, o por terceros, que se financien con recursos públicos federales, deberán alinearse con las disposiciones de la Estrategia Digital Nacional.

2. Ningún usuario debe emplear la identidad de otro usuario, y de la misma manera ninguno debe dar a conocer su contraseña o identificación a otro.

3. En cuanto a las reparaciones o mantenimientos de bienes de TIC, los usuarios deben saber que ocasionalmente el personal técnico de la División de Telemática tiene la autoridad para acceder al software instalado localmente y a sus datos. Sin embargo, el personal técnico de sistemas no puede acceder sin autorización en ninguna de estas eventualidades o usar esta información para propósitos diferentes a los institucionales.

4. Cualquier acceso de los usuarios a los sistemas de información será requerido a la División de Telemática, a través de una solicitud del Titular del Área (correo o memorándum), para la asignación de contraseñas y privilegios, según sus funciones.

5. Será considerado como malintencionado transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.

6. Ante un mantenimiento correctivo de los sistemas de información, la División de Telemática informará oportunamente a los usuarios el lapso probable de la interrupción del servicio.

7. Los usuarios no deberán modificar, reubicar o sustraer información propiedad del Instituto sin la debida autorización, ya que se considera como información confidencial.

8. Los enlaces o conexiones remotas no podrán ser usados para modificar, consultar o eliminar información, sin el permiso debidamente asignado.

Sección 3. Política del uso correcto de los Bienes de TIC

Objetivo

Establecer el uso correcto de los equipos de cómputo que el IMT asigna a los usuarios para el desarrollo de sus funciones, informando sobre los riegos asociados al uso inadecuado, a fin de garantizar la integridad de los equipos.

Ámbito de aplicación

La presente política aplica a todos los usuarios de bienes de TIC, incluyendo al personal que tenga servidores bajo su administración y resguardo.

Política

1. En el desempeño de sus actividades, es responsabilidad del personal el buen uso y resguardo de los bienes de TIC asignados.
2. El personal deberá firmar el formato “Resguardo de los bienes de TIC”, o bien, al realizar la devolución firmar el formato “Devolución de Bienes y Baja de Servicios de TIC”, que para tales efectos proporciona la División de Telemática.
3. Es responsabilidad del personal bloquear o finalizar sesión en su computadora cuando no la esté utilizando, esto con el fin de evitar accesos no autorizados al equipo ni a la información.
4. Las computadoras que, por necesidades del servicio deban ser utilizadas por más de una persona, deberán contar con perfiles de usuario personalizados, con el fin de preservar la confidencialidad e integridad de la información.
5. Todas las computadoras del IMT deberán tener instalado, actualizado y activado el software antivirus institucional, incluyendo servidores cuyo sistema operativo así lo permita.
6. El personal no deberá desinstalar, desactivar o interrumpir la actualización del antivirus institucional; así mismo no deberán instalar un antivirus diferente al institucional.
7. Es responsabilidad del personal cuidar que los medios de almacenamiento externo (USB y Discos Duros) estén libres de software malicioso; por tal motivo, deberá realizar una verificación por medio del antivirus institucional, cada vez que sean conectados.
8. Sólo el personal de la División de Telemática podrá realizar la descarga e instalación de software en los equipos asignados al personal del IMT, conforme a lo estipulado en la Política de uso de Software.
9. Sólo el personal de la División de Telemática podrá modificar la configuración en los equipos de cómputo asignados al personal del IMT.

10. Cuando el usuario requiera escalar o modificar las especificaciones de hardware de su equipo de cómputo asignado, deberá solicitarlo a la División de Telemática. Los usuarios no están autorizados en ninguna circunstancia a realizar modificaciones por su cuenta.
11. El personal no podrá realizar, acción alguna que vulnere la seguridad de la información de los bienes de TIC, tales como escaneo de puertos, pruebas de vulnerabilidad, etc.
12. Los servidores públicos que forman parte del IMT no podrán almacenar en los equipos de cómputo del IMT: juegos, música, video o cualquier archivo multimedia, o información personal, salvo que sea justificado para fines laborales.
13. Es responsabilidad del personal apagar su equipo de cómputo al término de su jornada laboral. Si necesita conectarse remotamente después del horario laboral, el Titular de su Área deberá gestionar la solicitud de acceso, a través de un memorándum dirigido al Titular de la División de Telemática.
14. Es responsabilidad del personal reportar a través del Sistema de Atención a Usuarios de TIC, cuando un bien telemático presente fallas. El personal no deberá intentar solucionarlo por cuenta propia, esto con el fin de no comprometer la integridad del bien.
15. La División de Telemática podrá proporcionar bienes de TIC con carácter temporal, a fin de atender eventos específicos fuera de las instalaciones del IMT. El Titular del Área deberá solicitarlo mediante memorándum dirigido al titular de la División de Telemática. El usuario deberá firmar el Formato “Resguardo de los bienes de TIC”, que para tales efectos proporcione la División de Telemática.
16. El usuario deberá otorgar las facilidades necesarias para que el personal de la División de Telemática realice los servicios de mantenimiento preventivo y correctivo a los bienes de TIC.
17. Ante un mantenimiento preventivo y correctivo a los bienes de TIC, la División de Telemática informará oportunamente a todo el personal del IMT el periodo programado para tal efecto.
18. El empleado no deberá ingerir bebidas y alimentos sobre cualquiera de los bienes de TIC, por lo que, en caso de un daño atribuible a un mal uso, la División de Telemática reportará a la Coordinación de Administración y Finanzas para proceder a resarcir el daño.

Sección 4. Política para Contraseñas

Objetivo

Establecer las actividades que se deben de tomar en cuenta en esta Política, creando contraseñas seguras, protegiéndolas y estableciendo la frecuencia de cambio, para proteger el acceso autorizado a sistemas, redes, aplicaciones y datos.

Ámbito de aplicación

La presente política aplica a todos los usuarios de bienes de TIC que requieran de una contraseña.

Política

1. Las contraseñas deberán estar conformadas por al menos 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales. No se debe utilizar el mismo carácter dos veces seguidas.
2. No debe contener datos personales del usuario.
3. La contraseña no debe contener palabras completas en ningún idioma, para evitar que sean descifradas por software dedicado a este fin.
4. No compartir las contraseñas.
5. Cambiar las contraseñas cada seis meses, a partir de la creación de la cuenta.
6. Para el caso de aplicativos (sistemas operativos, bases de datos o sistemas informáticos) o dispositivos (servidores, computadoras), cambiar las contraseñas que se les otorguen por primera vez.
7. No escribir ni dejar las contraseñas en lugares de fácil acceso físico o visual.

Sección 5. Política de Sitios Restringidos de TIC

Objetivo

Establecer las medidas de seguridad para controlar el acceso físico a las áreas restringidas (MDF's, IDF's y Centro de Datos) del IMT, con la finalidad de reducir los riesgos de accesos no autorizados que podrían exponerlo a pérdidas de información y a daños de recursos materiales.

Ámbito de aplicación

La presente política aplica a todas las personas que transiten por las instalaciones del IMT.

Políticas

1. El Responsable de Redes, Servidores y Centro de Datos es quien autorizará el acceso al sitio, así como el ingreso o egreso de cualquier bien de TIC o herramienta.
2. Queda prohibido el acceso a estas áreas, a todo personal no autorizado.
3. Los visitantes al sitio restringido deberán identificarse y ser acompañados por un empleado autorizado, durante su estancia.
4. Los pasillos de circulación interna deben mantenerse despejados de todo objeto.
5. Queda prohibido el ingreso o sustracción de cualquier tipo de bien de TIC, herramienta, etc., sin previa autorización por el Responsable de Redes, Servidores y Centro de Datos.
6. Queda prohibido introducir alimentos y bebidas.
7. Queda prohibido utilizar estas áreas como bodega u otros fines diferentes a su uso original.

Sección 6. Política del Servicio Telefónico

Objetivo

Establecer las mejores prácticas del servicio telefónico asignado a los servidores públicos que forman parte del IMT y colaboradores del IMT, concientizando sobre el uso racional y responsable del servicio, para mantener la comunicación dentro y fuera de las instalaciones.

Ámbito de aplicación

La presente política aplica a todos los usuarios del servicio telefónico del IMT.

Política

1. La División de Telemática asignará equipos de telefonía y extensiones telefónicas al personal del IMT, que por su función requiera de esta herramienta.

2. El servicio telefónico es exclusivamente para uso laboral.

3. El Titular del Área designará al personal a su cargo que requiera permisos de marcación externa al IMT, nacional y/o internacional, y deberá solicitarlo mediante un memorándum dirigido al Titular de la División de Telemática.

4. Es responsabilidad del usuario el resguardo de la contraseña, que es única, de uso personal e intransferible.

5. Es responsabilidad del usuario atender y depurar el buzón de voz que tenga asignado.

6. Ante cualquier evento que involucre a la operación de la infraestructura telefónica, la División de Telemática informará oportunamente al personal del IMT el lapso probable de la interrupción del servicio.

Sección 7. Política de Respaldos de Información

Objetivo

Garantizar la operatividad del servicio de respaldo de información que se realiza en el IMT, a través de lineamientos para la protección y recuperación de los datos.

Ámbito de aplicación

La presente política aplica a todos los empleados.

Políticas

1. El servicio de respaldo de información que proporciona la División de Telemática es estrictamente con fines laborales, y es obligatorio para todo el personal del IMT.

2. Los respaldos de información se realizarán con una periodicidad mensual y se conservarán durante el año en curso.

3. Los respaldos quedarán a resguardo de la División de Telemática y serán proporcionados sólo a solicitud del Titular del Área solicitante.

Sección 8. Política del uso de Software

Objetivo

Garantizar la operatividad del software comercial y desarrollado por el IMT, mediante lineamientos para su utilización, instalación y actualización, con el fin de asegurar la integridad de los equipos, evitar infracciones de propiedad intelectual, minimizar riesgos de seguridad y optimizar los recursos tecnológicos del Instituto.

Ámbito de aplicación

La presente política aplica a todos los usuarios de software del IMT.

Política

1. La solicitud de contratación de software comercial o desarrollado por el IMT, deberá ser gestionada por el Titular del Área solicitante, mediante los formatos “Solicitud de Software Comercial” o “Análisis de Requerimientos”, según corresponda.

2. La temporalidad del uso de software comercial o desarrollado por el IMT dependerá del tiempo previsto para el desarrollo del proyecto donde será utilizado; al término del proyecto, el software comercial deberá desinstalarse para que se pueda utilizar en otro proyecto institucional.

Del Software comercial:

1. La instalación del software se facilitará exclusivamente para el ejercicio de funciones laborales.

2. La instalación de software se realizará exclusivamente por personal de la División de Telemática y en equipos de cómputo oficiales.

3. El usuario solicitará la instalación del software a Atención a Usuarios de TIC, a través de la extensión telefónica correspondiente.

4. No se realizarán copias de software comercial para su entrega a las áreas, con el fin de evitar su reproducción ilegal.

5. La División de Telemática sólo instalará software contratado por el IMT, a excepción de las licencias de prueba (Shareware), libres (Freeware), o de convenios legales con otras instituciones.

6. El servicio de soporte técnico será proporcionado únicamente para software autorizado por el IMT.

7. La División de Telemática se reserva el derecho de desinstalar cualquier software no autorizado, en los equipos de cómputo del IMT.

8. Sin excepción alguna, queda prohibido duplicar, extraer o clonar software licenciado.

Del Software desarrollado por el IMT:

1. Se deberán de considerar los lineamientos del Manual de Desarrollo de Sistemas Informáticos del IMT.

2. Sin excepción alguna, queda prohibido duplicar, extraer o clonar software propiedad intelectual del IMT.

3. La solicitud de alta, baja o modificación de usuario, deberá ser gestionada por el Titular del Área solicitante con el Titular de la División de Telemática.

4. Cuando se presente una falla u oportunidad de mejora a una aplicación institucional, el usuario deberá reportarla al Administrador del Sistema.

Sección 9. Política del uso de Internet

Objetivo

Establecer actividades para el uso adecuado del servicio de Internet dentro del IMT, utilizando el recurso de manera ética y profesional, para contribuir a la productividad y eficiencia de los servidores públicos que forman parte del IMT.

Ámbito de aplicación

Aplica a todos los usuarios del servicio de Internet proporcionado por el IMT.

Políticas

1. El servicio de Internet será usado con fines estrictamente laborales.

2. La División de Telemática informará oportunamente del mantenimiento preventivo o correctivo a la infraestructura que soporta el servicio de Internet.

3. La División de Telemática, monitorea permanente la navegación de los usuarios en el servicio de Internet, y ante cualquier intento de violación, se enviará un reporte al Titular del Área del usuario, así como a la Coordinación de Administración y Finanzas, para que se realicen las acciones administrativas y legales correspondientes.

4. Está restringido el acceso a páginas de Internet con material obsceno y juegos.

5. La reproducción de video bajo demanda, redes sociales, páginas para gestión de compras en línea está restringido, salvo previa autorización al usuario por el Titular de su Área, a través de un memorándum dirigido al Titular de la División de Telemática. Dicho permiso estará vigente durante el año en curso.

6. Las conexiones por medio de FTP requeridas por el usuario, serán habilitadas y configuradas por el personal de la División de Telemática.

Sección 10. Política de la Administración de Sistemas de Información

Objetivo

Establecer las acciones de monitoreo continuo, actualizaciones regulares, respaldos e implementación de medidas de ciberseguridad, que los Administradores responsables de los sistemas de información del Instituto Mexicano del Transporte deben cumplir, para mantener, operar y proteger dichos sistemas.

Ámbito de aplicación

La presente política aplica a los Administradores responsables de los sistemas de información.

Políticas

1. Se deberán de considerar los lineamientos del Manual de Desarrollo de Sistemas Informáticos del IMT, relacionada a los Administradores de Sistemas.

2. El Administrador del Centro de Datos gestionará la reparación de fallas en el hardware donde residen los sistemas de información.

3. En caso de falla del sistema de información o el sistema operativo donde se aloja, la responsabilidad recae sobre el Administrador del Sistema.

4. El Administrador del Sistema deberá asegurarse de contar con el respaldo del código fuente y de su base de datos.

5. Las estructuras físicas y lógicas de los sistemas de información sólo podrán ser modificadas por el Responsable de Desarrollo de Sistemas Informáticos del IMT y el Administrador del Centro de Datos, a solicitud del Administrador del Sistema.

6. Ante un mantenimiento al Centro de Datos donde se alojan los sistemas de información, la División de Telemática informará oportunamente a los Administradores de sistemas el lapso probable de la interrupción del servicio.

7. El servidor donde resida un sistema de información, deberá tener activas sus bitácoras electrónicas (operación, error, accesos, registro de usuarios y actividades).

Sección 11. Política sobre el Manejo de Incidentes de Seguridad de la Información

Objetivo

Establecer las actividades básicas que se deben llevar a cabo ante un incidente de seguridad de la información en el IMT, desde la notificación del incidente hasta su apropiado manejo por la División de Telemática, conforme al Marco de Gestión de Seguridad de la Información, para preservar la información del Instituto.

Ámbito de aplicación

La presente política aplica a todos los usuarios de los servicios de TIC del IMT.

Políticas

1. Los usuarios deberán reportar a la División de Telemática, cualquier sospecha de un posible incidente de seguridad de la información.

2. Ante un incidente de seguridad de la información, la División de Telemática pondrá en práctica lo definido en el Marco de Gestión de Seguridad de la Información.

3. Ante un incidente que provoque una afectación en los bienes o servicios de TIC, la División de Telemática comunicará a la comunidad del IMT el tipo de daño y el tiempo estimado de resolución.

Sección 12. Política sobre el Borrado Seguro de la Información

Objetivo

Establecer las actividades necesarias para borrar de forma segura la información que así lo requiera, mediante herramientas de borrado irreversible, para garantizar que no sea utilizada por terceros o con fines diferentes a los que fue proporcionada.

Ámbito de aplicación

La presente política aplica a todos los usuarios del IMT.

Políticas

1. La División de Telemática será la única autorizada de realizar el borrado seguro de la información, en los siguientes casos:

    - Cuando el usuario ya no labore en el IMT.
    - Cuando alguna organización, ya sea pública o privada, solicite que se realice el borrado seguro de información prestada al IMT, al término del plazo del servicio o proyecto, previa autorización del Titular de Área.
    - Cuando existan bienes de TIC del IMT que vayan a ser retirados o cedidos a terceros.

Sección 13. Política sobre la Devolución de Bienes y Baja de Servicios de TIC

Objetivo

Establecer las actividades que los usuarios deben realizar para la devolución de bienes de TIC que les fueron asignados, incluyendo: la devolución física de los equipos, la baja de servicios, así como la verificación de credenciales, para asegurar la recuperación de los recursos de TIC.

Ámbito de aplicación

La presente política aplica a todos los usuarios que concluyen su relación con el IMT.

Políticas

1. El usuario deberá solicitar a la División de Telemática el formato de “Devolución de Bienes y Baja de Servicios de TIC”, que incluye:
    - Bienes de TIC: se recogerá el equipo al menos un día antes de la entrega de su baja, y quedará a resguardo de la División de Telemática.
    - Cuentas de usuario: a la entrega de su baja, se deshabilitará de los sistemas y servicios de TIC en los que esté involucrado.
    - Material documental (Centro de Información y Documentación): el usuario entregará el material documental prestado, el cual deberá estar en buen estado, o ser reemplazado por otro similar en buenas condiciones, al menos un día antes de la entrega de su baja, el cual quedará a resguardo de la División de Telemática.
    - Activos de información: el respaldo de la información se realizará conforme a la política de respaldos, y le será proporcionado al Titular del Área.
    - Sistemas de Información Administrados: el Administrador responsable del Sistema de Información entregará las credenciales a la División de Telemática, al menos dos semanas antes de su baja, misma que serán verificadas con el sistema funcionando.

2. En caso de que el usuario no cumpla con alguno de los puntos anteriores, según corresponda, la División de Telemática no entregará la carta de “Devolución de Bienes y Baja de Servicios de TIC”.

3. Una vez firmado, el formato se entregará a la Oficina de Capital Humano, con copia al usuario (acuse de recibo).

IX. EMISOR

Fecha: 20240906

Elaboró:	Firma:
Manuel Alegría López Gestión y Desarrollo de los Sistemas Informáticos y Base de Datos	
Sandra Victoria Álvarez Granados Administración de Sistemas Informáticos y Conmutadores	
José Antonio Fernández Rico Redes, Servidores y Centro de Datos	
Héctor Huicochea Pérez Administración y Gestión de la Mesa de Servicios	
Emilio Mauricio Cruz Desarrollo de Sistemas Informáticos, Web y Base de Datos	
María Ariadna Sánchez Loo Desarrollo de Proyectos	
José Carlos Ugalde Chehín Administración de Proyectos y Cursos Virtuales	
Aarón Isaí Villanueva Carvallo Sistemas de Comunicación y Seguridad de la Información	

Revisó:

MGP. Perla Jasivy Vargas Carrillo
Jefa de la División de Telemática

Autorizó:

Dr. Alberto Mendoza Díaz
Director General