DIRECCIÓN DE INFORMÁTICA

Políticas de Seguridad Informática y Tecnologías de la Información

Guatemala, agosto 2022

ÍNDICE

INTRODUCCIÓN

La información es un activo de alto valor para el Instituto de Fomento Municipal. A medida que los procesos de la entidad se hacen más dependientes de la información y de la tecnología que la soporta, se hace necesario contar con reglas de alto nivel que permitan el control y administración efectiva de los datos.

El manual de políticas contiene lineamientos y directrices tanto de seguridad de la información como de seguridad informática. La adopción de los dos enfoques busca afrontar integralmente las amenazas que pueden comprometer a la información de la Institución.

AUTORIZACIÓN (RESOLUCIÓN DE JUNTA DIRECTIVA)

GOBIERNO de GUATEMALA
DR. ALEJANDRO GIAMMATTEI

INSTITUTO DE FOMENTO MUNICIPAL -INFOM-

LA INFRASCRITA SECRETARIA DE LA JUNTA DIRECTIVA DEL INSTITUTO DE FOMENTO MUNICIPAL -INFOM-. ----------

C E R T I F I C A:

Tener a la vista el Acta número setenta guion dos mil veintidós (70-2022) de la Sesión Ordinaria de la Junta Directiva del Instituto de Fomento Municipal, celebrada el treinta de agosto del año dos mil veintidós; la que en su parte conducente del Punto Sexto (6to.) copiado literalmente dice: "...RESOLUCIÓN DE JUNTA DIRECTIVA NÚMERO DOSCIENTOS TREINTA GUION DOS MIL VEINTIDOS (230-2022). LA JUNTA DIRECTIVA DEL INSTITUTO DE FOMENTO MUNICIPAL, deliberó de forma y de fondo el asunto sometido a su conocimiento y, **CONSIDERANDO:** Que la Ley Orgánica del Instituto de Fomento Municipal, establece que el Instituto es una entidad estatal, que goza de autonomía funcional, patrimonio propio, personalidad jurídica y plena capacidad para adquirir derechos y contraer obligaciones en materia de su competencia, el que se rige por su Ley Orgánica, disposiciones legales aplicables, reglamentos internos y acuerdos que emita la Junta Directiva. **CONSIDERANDO:** Que el Gerente del Instituto a través del oficio GER guion mil noventa y ocho guion dos mil veintidós (GER-1098-2022) del diecisiete de agosto de dos mil veintidós, trasladó para consideración y aprobación de la Junta Directiva, las Políticas de Seguridad Informática y Tecnologías de la Información de la Dirección de Informática, las cuales fueron realizadas en cumplimiento a la recomendación de la Dirección de Auditoria Interna. **CONSIDERANDO:** Que a través del Dictamen AJ guion ciento dieciséis guion dos mil veintidós (AJ-116-2022) del once de agosto de dos mil veintidós, la Dirección de Asesoría Jurídica dictaminó que el Manual de Organización y Funciones de la Dirección de Informática, se ajusta a las normas legales aplicables, siendo legalmente procedente su aprobación. **POR TANTO**: La Junta Directiva del Instituto de Fomento Municipal, en ejercicio de las atribuciones que le confieren los artículos 15 y 23 literal l) del Decreto número 1132 del Congreso de la República

1

8a Calle 1-66 Zona 9 Guatemala, C.A
PBX: 2317-1991

Resolución No. 230-2022

de Guatemala, Ley Orgánica del Instituto de Fomento Municipal; por unanimidad, **RESUELVE: I.** Aprobar **LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA DIRECCIÓN DE INFORMÁTICA DEL INSTITUTO DE FOMENTO MUNICIPAL**, que obra en el documento adjunto a la presente. **II.** Esta resolución surte efectos a partir de su notificación. **III.** Se instruye a la Gerencia para que, a través de la Secretaría General del Instituto de Fomento Municipal, proceda a realizar las notificaciones correspondientes. **IV.** Notifíquese ..." ----------

Y, para remitir a donde corresponde se certifica el presente punto de acta, en la ciudad de Guatemala, el treinta de agosto del año dos mil veintidós. ----------

2

INSTITUTO DE FOMENTO MUNICIPAL - GUATEMALA, C. A. - Secretaría de la Junta Directiva

Licda. Lissgrid Yanira Alarcón Valdez
Secretaria de Junta Directiva

INSTITUTO DE FOMENTO MUNICIPAL - PRESIDENTE - GUATEMALA, C. A.

Vo. Bo. Lic. Oscar Martín Molliner Estrada
Presidente de Junta Directiva

OBJETIVO DEL MANUAL

Objetivo General

Formular y actualizar las políticas de seguridad informática para toda la entidad. Revisando, aprobando y procurando el cumplimiento de las políticas a través de la formulación y revisión de las mismas.

Objetivos específicos

- Promover comportamientos de seguridad responsables.
- Exhortar las actuaciones profesionales y éticas.
- Promover una cultura positiva para la seguridad.
- Tener un enfoque basado en los riesgos Institucionales.
- Promover la mejora continua de los servicios informáticos
- Proteger la información digital de la Institución.
- Evaluar las amenazas actuales y futuras de la información.
- Proteger la Institución de accesos no autorizados a los servicios informáticos.
- Soportar el actuar de la entidad con buenas prácticas en la tecnología actual.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad.

ÁMBITO DE APLICACIÓN

El presente manual contiene lineamientos de observancia obligatoria, aplicables a todas las unidades y áreas de esta Institución que sean dependientes de las tecnologías de la información administradas por parte de la Dirección de Informática. Asimismo, el alcance de los lineamientos contenidos en este manual se extenderá a todas las demás unidades y áreas que puedan ser creadas posterior a la aprobación de este manual.

BASE LEGAL

El artículo 31 de la Ley Orgánica del Instituto de Fomento Municipal contenida en el Decreto 1132 del Congreso de la República, el Instituto contará con las secciones indispensables para el eficaz desarrollo de sus operaciones y finalidades. La Junta Directiva acordará la creación de las secciones necesarias para la buena marcha de los servicios de la Institución. Asimismo, el artículo 32 del referido cuerpo legal, establece que cada sección tendrá un jefe nombrado por Junta Directiva a propuesta del Gerente, y el personal indispensable para su buen funcionamiento. El reglamento de la Institución determinará normas de operación de cada sección y las responsabilidades y atribuciones del personal de las mismas.

NORMAS GENERALES

La Dirección de Informática, de conformidad con la legislación positiva y vigente, rige su funcionamiento según lo preceptuado en los siguientes instrumentos jurídicos:

- Constitución Política de la República de Guatemala.
- Ley Orgánica del Instituto de Fomento Municipal, Decreto 1132 del Congreso de la República.
- Reglamento de Relaciones Laborales del Personal del Instituto de Fomento Municipal, Acuerdo Gubernativo Número 234-86.
- Código de Trabajo y sus reformas, Decreto 1441 del Congreso de la República de Guatemala.
- Normas Generales de Control Interno Gubernamental emitidas por la Contraloría General de Cuentas, emitidas en junio de 2006.
- Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República de Guatemala.
- Reglamento de la Ley para el reconocimiento de las comunicaciones y firmas electrónicas, Acuerdo gubernativo 135-2009.
- Manual de Organización y Funciones del Instituto de Fomento Municipal, Aprobado mediante Resolución de Junta Directiva número 227-2016
- Acuerdo número 317-2021, aprobación del uso de correo electrónico registrado bajo el dominio infom.gob.gt como herramienta oficial de comunicación de la institución.

Políticas de Seguridad Informática y Tecnologías de la Información

Seguridad de la información de la Institución

Para garantizar la fiabilidad de la información que guardan los sistemas informáticos de la Institución, se implementarán eficientemente políticas de grupo. Las políticas de grupo no son más que un conjunto de reglas implementadas, mediante cambios efectuados en el registro que se activan al iniciar el equipo o cuando un usuario inicia su sesión de trabajo. Las políticas entran a formar parte del entorno de usuario e imponen restricciones sobre las acciones de dicho usuario.

Estas políticas también nos permiten establecer de forma centralizada múltiples aspectos de la configuración que reciben los usuarios cuando se conectan a un equipo del dominio. Estos aspectos incluyen, entre diversos tipos: configuraciones del registro, políticas de seguridad, instalación automática de software, ejecución de scripts, configuración de navegación, redirección de carpetas locales a recursos de red, etc.

A continuación, se dividirán las distintas políticas generales de seguridad informática y tecnologías de la información, según su naturaleza de aplicación.

Políticas de red, directivas y configuración de equipos

Descripción de las Políticas

Dentro de las políticas de grupo a implementar en el directorio activo del dominio de la Institución, se encuentran las directivas aplicables a los equipos y las directivas aplicables a los usuarios.

La configuración del equipo agrupa todos aquellos parámetros de configuración que pueden establecerse a nivel de equipo y a nivel usuario. Cuando una política de grupo afecta a un equipo, todas aquellas políticas de equipo que el administrador haya configurado se aplicarán al equipo cada vez que se inicie. Cuando una política de grupo afecta a un usuario, todas aquellas políticas de

usuario que el administrador haya configurado se aplicarán cuando dicho usuario inicie una sesión local (en cualquier equipo del dominio).

La jerarquía de políticas en cada uno de ellos se subdivide en tres grupos:

- Configuración de software: contiene la configuración, bien del equipo o bien de usuario, de la instalación automática de software.
- Configuración de Windows: contiene la configuración de ciertos parámetros de Windows, como parámetros de seguridad o scripts, para el equipo o para el usuario.
- Plantillas administrativas: contiene las políticas y configuraciones que se guardan en el registro de Windows, para el equipo o para el usuario.

Es decir, en muchos casos, la misma política existe en ambos subárboles (equipo y usuario), aunque generalmente en cada caso con significados y parámetros distintos. En ese orden, bajo configuración del equipo-configuración de Windows-scripts podemos encontrar los scripts que deben ejecutarse cada vez que el equipo se inicia o detiene, mientras que bajo configuración de usuario-configuración de Windows-scripts se encuentran los scripts que deben ejecutarse cada vez que el usuario inicia o finaliza una sesión local.

A continuación, se exponen los grupos de políticas más importantes que pueden configurarse mediante políticas de grupo, independientemente de su ubicación concreta dentro de la jerarquía.

Plantillas administrativas

Este grupo contiene todas las configuraciones de políticas basadas en el registro de Windows, incluyendo aquellas que controlan el funcionamiento y apariencia del escritorio, de los componentes de Windows y de algunas aplicaciones que utilizan estas políticas.

Configuraciones de seguridad

En este apartado se encuentra la configuración de muchos de los aspectos de seguridad que pueden establecerse en un sistema Windows o superior.

En concreto, y concentrándonos en los aspectos de seguridad a nivel de equipo podemos destacar los siguientes aspectos:

- Políticas de cuentas: se pueden configurar todos los aspectos sobre el plan de cuentas tales como la caducidad de contraseñas, bloqueo de cuentas, configuración de seguridad, etc.
- Políticas locales: bajo este apartado se encuentran las configuraciones que corresponden a la denominada "directiva local", es decir, la configuración de la auditoría, la asignación de derechos y privilegios de usuario y las opciones de seguridad.
- Registro de eventos: aquí se controla el registro de eventos en los registros de aplicación, seguridad y sistema, que posteriormente pueden visualizarse con la herramienta visor de sucesos.

Instalación de software

- Mediante este apartado se puede asignar y/o publicar aplicaciones a equipos o a usuarios en el dominio:
- Asignar una aplicación significa que los usuarios que necesiten determinado programa, estará disponible en su escritorio sin necesidad de que un administrador la instale. Cuando se asigna una aplicación a un usuario o equipo, se crea una entrada para ella en el menú de inicio y se configura el registro adecuadamente. La primera vez que el usuario ejecuta la aplicación, ésta es automáticamente instalada en el equipo cliente.
- Publicar una aplicación a un equipo o usuario le da la oportunidad al usuario de instalar dicha aplicación bajo demanda (a voluntad), pero no se realiza

ninguna acción automática en el equipo (no se modifica el menú de inicio ni el registro). La lista de aplicaciones publicadas para un usuario aparece en el panel de control, bajo la herramienta de añadir/eliminar programas, desde donde pueden ser instaladas.

Guiones (Scripts)

Bajo este apartado, se pueden asignar scripts a equipos o usuarios. En concreto, existen cuatro tipos de scripts principales:

- Inicio (equipo): se ejecuta cada vez que el equipo arranca.
- Apagado (equipo): se ejecuta cada vez que el equipo va a detenerse.
- Inicio de sesión (usuario): se ejecuta cada vez que el usuario inicia una sesión interactiva (local) en un equipo.
- Cierre de sesión (usuario): se ejecuta cada vez que el usuario finaliza una sesión interactiva en un equipo.

En todos esos casos, los scripts pueden implementarse en cualquiera de los lenguajes que entiende el soporte de scripts independiente del lenguaje de Windows 7, Windows 10, o Windows scripting host. Actualmente existe soporte para visual basic scripting edition, java script, PERL y los tradicionales archivos por lotes MS-DOS característico de los sistemas operativos de Microsoft Windows. El comportamiento de los scripts puede perfilarse mediante algunas políticas que se sitúan en el apartado de plantillas administrativas.

Redirección de carpetas

Este grupo de políticas permite redirigir la ubicación local predefinida de ciertas carpetas particulares de cada usuario (como "Mis documentos" o el menú de inicio) a otra ubicación, bien sea en la misma máquina o en una unidad de red.

Un ejemplo útil de redirección seria que la carpeta "Mis documentos" apuntara a un directorio personal de cada usuario en la red, como por ejemplo el recurso

\\servidor\home\%usemame%. Esta aproximación resulta más útil que conectarle a dicho usuario ese recurso a una unidad de red, puesto que muchas aplicaciones abren automáticamente la carpeta "Mis documentos" para buscar los archivos personales de ese usuario. Para que dicha redirección funcione correctamente, es necesario que el usuario que recibe la redirección sea el propietario de la carpeta compartida.

Directivas a implementar

Después de haber descrito muy generalmente el alcance de las políticas de grupo, a continuación, se describen las políticas a aplicar en el directorio activo de la Institución.

Directivas para el usuario

- **Inicio de sesión:** El usuario de red del directorio activo, podrá registrarse en una sola estación de trabajo; si el usuario por razones plenamente justificables, necesita ingresar a otra estación de trabajo, deberá enviar nota a la DI con el visto bueno del jefe inmediato superior para la configuración de dicho acceso.
- **Contraseñas aceptables:** La principal forma es utilizar contraseñas con combinaciones de minúsculas y mayúsculas, números mezclados con texto, símbolos como &, $ o %, etc., y con un mínimo de 6 caracteres. Por supuesto, no se deben colocar contraseñas simples como “Guatemala” o “Metallica”, nombres propios, combinaciones débiles como “Quezada1” o nombres de lugares, actores, personajes de libros, deportistas. Por último, es necesario recordar que para que una contraseña sea aceptable obligatoriamente ha de cumplir el principio "*KEEP IT SECRET*" que quiere decir manténgala en secreto.
- **Caducidad de contraseñas:** La idea de esta directiva es proteger las contraseñas de los usuarios dándoles un período de vida máximo

de 45 días, una contraseña solo va a ser válida durante este tiempo, pasado el cual expirará y el usuario deberá cambiarla. Además del tiempo de caducidad se suma el historial de contraseñas, obligando al usuario a utilizar una contraseña distinta a la que caducó para que dicha directiva prevenga más que problemas con las contraseñas. De esta forma un usuario que conozca o llegue a conocer la contraseña de otro usuario solo podrá utilizarla hasta que el sistema nos obligue a cambiarla. Cabe recalcar que si tras el período de cambio obligatorio, la contraseña permanece inalterada, la cuenta se bloquea y es necesario solicitar necesitando solicitar a la DI desbloquear la misma.

- **Bloqueo de usuarios por autenticación fallida**: Se considera necesario el bloqueo de cuentas de usuario después de 3 intentos fallidos de autenticación, esto con el fin de evitar que usuarios malintencionados intenten repetidamente hacer ingreso con cuentas de otros usuarios, necesitando solicitar a la DI desbloquear la cuenta.
- **Deshabilitar el acceso al panel de control:** el principal objetivo es proteger al sistema de modificaciones y mantener un entorno estándar, asegurando así la funcionalidad de las aplicaciones y sistemas operativos de los equipos en el Dominio de la Institución.
- **Deshabilitar el acceso al entorno de Red:** directiva con el objetivo primordial de evitar que usuarios malintencionados o personal ajeno a la DI, realicen cambios en la configuración de red de los equipos, evitando así la pérdida de comunicación.
- **Deshabilitar la instalación de software:** esto es importante desde el punto de vista que, se evita que los usuarios agreguen software que generen ocio y pérdida de tiempo y a la vez se evita la instalación de software pirata o no licenciado.
- **Deshabilitar la ejecución de software:** se busca deshabilitar la ejecución de programas específicos tales como juegos para evitar el

ocio y herramientas administrativas a las cuales solo los técnicos en soporte tendrán acceso como herramientas de trabajo.

- **Estandarización del Escritorio:** Con esto se busca evitar que el usuario modifique las configuraciones de presentación de su perfil de trabajo y mejorar el rendimiento de los equipos.

Políticas de acceso físico al área de la dirección de informática

Seguridad en las instalaciones de la DI

Para que cualquiera de las políticas de seguridad enfocadas a los datos sea funcional, también es necesario garantizar la seguridad en cuanto a acceso a las instalaciones físicas de la DI, dado que, es en este lugar donde se resguardan los servidores, bases de datos y sistemas, así como todos los equipos de telecomunicaciones.

El acceso a la DI deberá ser restringido, solo para personal autorizado, contándose con un registro de entradas y salidas de terceras personas (incluye a las personas de mantenimiento del aire acondicionado, los visitantes y el personal de limpieza). Estos y cualquier otro personal ajeno a la instalación deben ser:

- Identificarse plenamente sobre su procedencia.
- Observar las actividades realizadas durante el acceso.
- El personal de mantenimiento y cualquier otra persona ajena a la DI se debe identificar antes de ingresar.
- La permanencia dentro de las instalaciones de la DI, de cualquier persona ajena a la misma deberá estar siempre acompañado por algún colaborador de DI.

Al acceso al área de servidores debe estar totalmente restringida. Únicamente debe estar autorizado el ingreso el director de Informática y a quienes por la

naturaleza de sus funciones necesiten ingresar a esta área, siempre y cuando lo autorice el director de Informática y que su permanencia sea reportada.

Políticas de comunicación interna y externa

Políticas del servicio

La Institución, a través de la DI, proveerá a sus colaboradores cuentas de correo electrónico, según la naturaleza de sus actividades y funciones, con el objeto de darles apoyo en su trabajo diario. Dichas cuentas de correo electrónico están asignadas a los colaboradores, pero son propiedad de la Institución. Para regular su uso, se adecuarán políticas adicionales en el **Manual de Normas y Procedimientos** de la DI los cuales ampliarán el alcance de estas políticas y se armonizarán en beneficio de otorgar la calidad del servicio de comunicación interno y externo a través de este medio.

Acceso a los servicios y responsabilidad

La utilización de los recursos de red y de información está abierta a todas las direcciones y/o áreas que la Institución bajo las políticas de acceso definidas en el contexto del presente documento y a otras personas a las que la Institución desee extender los privilegios de acceso, dadas las condiciones de disponibilidad de recursos, servicios y aprobación por escrito de la autoridad superior.

Cada empleado de la institución es el único responsable de las actividades realizadas con la cuenta de correo electrónico, así como el adecuado uso del buzón de correspondencia.

Los mensajes que se envíen por correo, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, los de esta o cualquier otra Institución. Además de dar estricto cumplimiento a la

legislación vigente, en el caso de cometer faltas o ilícitos sancionables por el derecho sustantivo.

Uso del correo electrónico

El correo electrónico es un medio de comunicación aprobado mediante Acuerdo número 317-2021, por lo que se considera parte de los canales y medios oficiales de comunicación de la Institución. El uso del correo electrónico y documentos adjuntos se limita a las funciones y atribuciones propias de cada puesto. Este medio de comunicación no debe utilizarse para comunicaciones personales sin relación al desempeño de responsabilidades de cada colaborar que cuente con una cuenta debidamente asignada a su persona. En el uso del correo electrónico deberán de observarse las siguientes generalidades:

- Su uso continuo no deberá afectar el rendimiento del servicio de correo electrónico de la Institución.
- En su uso como medio de comunicación institucional, no se deberá de interferir en las labores propias del usuario. Es decir, no debe ser una herramienta de distracción.
- Se permite el envío de archivos adjuntos siempre que el contenido de los mismos tenga una relación directa con el desempeño del puesto del usuario de la cuenta de correo y que estos se encuentren bajo el tipo de archivos permitidos contemplados en el Manual de Normas y Procedimientos de la DI.

Prohibiciones al uso del correo electrónico

Esta completamente prohibido realizar cualquiera de las actividades definidas a continuación:

- Iniciar o dar seguimiento a "cadenas de correo" que contengan mensajes que no sean relacionados al trabajo.

- Distribuir, ya sea de forma masiva o no, mensajes con contenidos inapropiados para la Institución.
- Falsificar el origen o el encabezado de los correos electrónicos.
- El envío de correos electrónicos masivos sin autorización previa y/o la suscripción a listas de distribución de correo electrónico que no tengan relación a las funciones laborales del empleado.
- Utilizar la cuenta de correo para perder deliberadamente el tiempo en horarios de trabajo, por medio del envío y/o lectura de mensajes ajenos a la actividad diaria que se desarrolla; es decir, mensajes de entretenimiento y con archivos adjuntos, tales como, presentaciones o imágenes, en especial aquellas que atenten contra la moral (entiéndase entre otros: contenido pornográfico, violencia y sexo).
- Todas las demás reguladas en las leyes sustantivas vigentes que constituyan faltas o delitos.

Privacidad

Todos los usuarios conocen y aceptan las cláusulas de privacidad que se presenta a continuación, por lo que no constituirá violación de su privacidad cualquier tema contemplado.

Las Autoridades Superiores están facultadas para solicitar en base a una investigación oficial, que la persona permita que sea revisado su buzón de correo electrónico y carpetas personales de correo. De denegarse dicha revisión, se procederá a resolver conforme a derecho corresponda, la revisión del buzón de correo electrónico.

Sanciones

Las autoridades superiores y la DI son los únicos autorizados para administrar y controlar la utilización de este recurso. Cualquier quebranto de las normas establecidas en el presente documento será motivo de sanción, que implicará la suspensión del acceso al servicio y reporte a la dirección de Recursos

Humanos. La cancelación parcial o definitiva del acceso a este servicio estará sujeta a este criterio, por lo que cualquier reactivación deberá solicitarse por escrito a la DI con visto bueno, firma y sello de las autoridades superiores.

Normas y políticas de uso de hardware y software

La tecnología de la información (TI) contribuye a superar los niveles de productividad y eficiencia de la Institución, siendo la DI la encargada de proveer los servicios necesarios para brindar al usuario el máximo apoyo en cuanto a sistematización, mecanismos de consulta y solución de problemas computacionales. Para ello es necesario que el usuario conozca las políticas y normas establecidas por la DI, las cuales deben ser definidas clara y explícitamente para poder administrar los recursos de TI de forma eficiente o en su momento poder deducir responsabilidades.

Políticas generales de Hardware y Software

El usuario que recibe cualquier hardware y/o software necesario para el desempeño de sus funciones, es el único responsable del mismo.

Es total responsabilidad y obligación del usuario lo siguiente:

- Dar cumplimiento a todas las normas y políticas vigentes.
- Preservar el estado de los equipos, periféricos y cualquier otro elemento de soporte que se le entregue.
- Utilizar adecuadamente el software que se le ha autorizado e instalado.
- Preservar la veracidad de los datos en los sistemas a que se le de acceso.
- Informar a la DI, cualquier cambio relacionado al hardware y/o software; cambio de ubicación física del equipo; y cambio de puesto o atribuciones (esto hace variar los accesos a sistemas, así como los perfiles de acceso).

- Utilizar su usuario y contraseña con total discreción, ya que el usuario es el único responsable del estado o contenido de los registros de cualquier sistema, donde sea evidente el acceso al registro por medio del código relacionado a su usuario.

Es responsabilidad de la DI, velar por el buen funcionamiento de los servicios de tecnología e informática que se presten dentro de la Institución; así como brindar a los usuarios el soporte técnico necesario en el uso de herramientas de software y hardware, así como también lo es en el soporte de los diversos sistemas en uso por las unidades del Instituto de Fomento Municipal.

Normas generales en el uso de Software y Hardware

El objetivo de estas normas es entregar las reglas adecuadas que permitan lograr un trabajo más seguro y eficiente, facilitando tanto las tareas del usuario, como las del personal de soporte de la DI, sustentando así la productividad de ambos.

Estas normas deben ser conocidas y respetadas por todos. La infracción de alguna de ellas puede acarrear consecuencias negativas para el usuario. Por tanto, el usuario será responsable de conocer y respetar estas normas así corno de las consecuencias que deriven del no cumplimiento de las presentes políticas. Para tal efecto, se establecen una serie de condiciones relacionadas con el uso de software y hardware.

La DI es la única autorizada para:

- Efectuar mantenimientos preventivos y/o correctivos en los equipos o instalar software y sistemas que los usuarios requieran.
- Solo se le dará mantenimiento a los equipos que pertenezcan a la Institución y estén debidamente identificados con su respectivo número de inventario.

- Los usuarios deberán cuidar física y lógicamente los recursos computacionales existentes, pensando que estos están al servicio de todos.
- No se recomienda manipular alimentos o bebidas cerca o sobre los equipos de cómputo, ya que cualquier derrame podrá causar daños al mismo.
- No está permitida la utilización de los equipos de cómputo con fines recreativos ni con fines particulares.
- El usuario no deberá abrir los equipos de cómputo, como tampoco remover o cambiar componentes de los equipos.
- Evitar prestar o intercambiar los equipos de cómputo.
- En ningún momento se deberán instalar equipos o periféricos que de alguna manera interactúen con la infraestructura o equipos de tecnología e informática de la Institución.

Normas generales Software

El equipo de cómputo que sea entregado al usuario contendrá el software básico, para el desempeño de sus funciones. Siendo el software básico, el definido por la DI. Cualquier otro software que requiera el usuario, deberá ser solicitado por medio de oficio.

En cualquiera de las formas utilizadas, la solicitud como mínimo deberá incluir:
Nombre completo del usuario.

- Unidad donde labora.
- Puesto o funciones que desempeña.
- Justificación válida y que relacione el desempeño de las actividades laborales del usuario.
- Visto bueno, firma y sello del jefe inmediato o en su defecto por la autoridad superior.

Toda solicitud ingresada a la DI, será evaluada y de considerarse a lugar, se procederá a la instalación del software solicitado siempre que la Institución cuente con las respectivas licencias para la instalación y uso del mismo. Si la DI considerara a lugar la solicitud, pero no existiere el licenciamiento correspondiente dentro del inventario de software licenciado de la Institución, entonces será responsabilidad del interesado, tramitar con la autoridad superior la autorización de compra, misma que de ser autorizada deberá trasladarse al área de Compras de la Institución, quienes deberán basarse en las especificaciones técnicas que la DI defina y además cumplir con todos los procedimientos legales, presupuestarios o cualquier otro que la Institución establezca.

Tras la instalación de un software determinado, se deberán observar y hacer cumplir los siguientes aspectos:

- El usuario deberá mantener los archivos de su equipo ordenados.
- La instalación y pruebas técnicas de software solo podrán ser efectuadas por la DI.
- En todo momento deberá respetarse la propiedad intelectual, por lo que no se podrá copiar o redistribuir software sin la autorización del fabricante o de la DI si corresponde.
- Toda instalación de software y/o sistema no autorizado por la DI, que provoque el inadecuado funcionamiento del equipo o de aplicaciones autorizadas, será responsabilidad del usuario.
- Todo software que no haya sido instalado con autorización expresa de la DI, podrá ser eliminado sin previo aviso y sin responsabilidad alguna para la DI por los datos o información que el usuario reclame como perdidos.

Prohibiciones para los Usuarios

- Copiar o "piratear" software, a menos que este sea de domino público (gratuito; licencia pública). La violación a esta prohibición es un acto ilícito, que puede causar sanciones legales para la Institución.

- Alterar software y/o sistemas que se encuentran a su disposición.
- Cambiar la configuración de los equipos, que ha sido determinada por la DI.
- Ninguno de los programas que se encuentran registrados deben ser instalados en otro sistema o computador diferente de aquel donde este se encuentre instalado, licenciado y autorizado por la DI.
- Instalar software no autorizado por la DI, ya que esto podría en algún momento causar daños a los equipos informáticos y/o redes por infección de virus, spyware, adware o algún otro; lo que podría ocasionar pérdidas importantes de información, atrasos y en el peor de los casos, daños al hardware del equipo.
- Realizar la actualización de software sin la autorización de la DI.
- Copiar y/o almacenar en el equipo que le fue asignado cualquier tipo de archivo que no tenga relación a las funciones laborales del usuario: por ejemplo: archivos de sonido, videos, imágenes, juegos o cualquier otro de carácter personal.
- Eliminar información digital contenida o siendo la misma, documentos de texto, hojas de cálculo, documentos audiovisuales y todo archivo que contenga información relativa al Instituto de Fomento Municipal, quien es propietaria de toda la información producida y contenida en los equipos y sistemas informáticos. El incurrir en esta prohibición conllevará la comisión de delitos contenidos en la legislación penal vigente de este país.

Sanciones

Cualquier infracción a las normas o políticas establecidas en el presente documento será motivo de sanción administrativa, por lo que es obligación de la DI, elaborar los informes correspondientes a la Dirección de Recursos Humanos, quienes en su momento determinarán la sanción correspondiente basándose en la gravedad de la falta, recurrencia o cualquier otro criterio administrativamente válido.

TERMINOLOGÍA TÉCNICA

Licencia pública: Es una licencia de derecho de autor ampliamente usada en el mundo del software libre y código abierto, y garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software.

Piratear: Aprovecharse del trabajo o de las obras de otros, especialmente copiando programas informáticos u obras de literatura o de música sin estar autorizado legalmente para hacerlo.

Script: Secuencia de comandos o guion es un término informal que se usa para designar a un programa relativamente simple.

Software: Conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.

Hardware: Conjunto de componentes físicos de los que está conformado el equipo.

Redirección: Reenvío automático que se utilizan para diversos fines, como la reubicación de un sitio web en un nuevo dominio o el mantenimiento de un servidor.

MS-DOS: Es un sistema operativo sin interfaz gráfica que confiaba puramente en una interfaz de línea de comandos para funcionar, con un total de 109 comandos con los que movernos por el sistema y utilizar sus capacidades, que en la mayoría de casos pasaban por ejecutar otras aplicaciones.

Visual Basic: Visual Basic es un lenguaje de programación dirigido por eventos, desarrollado por Alan Cooper para Microsoft. Este lenguaje de programación es un dialecto con importantes agregados.

Plantilla: Modelo o patrón que proporciona los elementos básicos para crear un tipo determinado de documento o archivo. Además de ello, su uso se orienta principalmente en ahorrar tiempo y facilitar la elaboración del documento ya que pueden contener texto, imágenes, formatos y estilos, además de otras características.

Directiva de grupo: Es un conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo. Directiva de grupo proporciona la gestión centralizada y configuración de sistemas operativos, aplicaciones y configuración de los usuarios.

Siglas

- **INFOM:** Instituto de momento municipal.
- **DI:** Dirección de Informática.
- **TI:** Tecnología de la información.