MUNICIPALIDAD DISTRITAL DE LA ESPERANZA

CREADO EL 29 DE ENERO DE 1965 - LEY N° 15418

Jr. Carlos María de Alvear N° 999 - Teléfonos: 272478 - 483330 - 272345 - 271744

TRUJILLO - PERÚ

"AÑO DE LA UNIDAD, LA PAZ Y EL DESARROLLO"

RESOLUCION DE ALCALDIA N° 0575-2023-MDE

La Esperanza, 08 de mayo del 2023

VISTO, el Informe N°051-2023-MDE/GM-SGIS, Informe N°757-2023-MDE/GRH y el Informe Legal N° 0410-2023- MDE/GAJ, sobre **APROBACIÓN DE DIRECTIVA N° 003-2023-MDE DIRECTIVA DE USUARIOS Y SEGURIDAD INFORMATICA"**, y;

CONSIDERANDO:

Que, el Artículo 194º de la Constitución Política del Estado, modificada por la Ley de Reforma Constitucional Ley Nº 27680, y la Ley de Reforma Ley 28607, prescribe que: "Las Municipalidades provinciales y distritales son órganos de gobierno local con autonomía política, económica y administrativa en los asuntos de su competencia".

Que, según **Informe N°051-2023-MDE/GM-SGIS**, de fecha 10 de marzo del 2023, emitido por el **Ing. José Bernardo Castro Gonzales** en su calidad de Sub Gerente de Informática y Sistemas, quien hace llegar la propuesta de **"DIRECTIVA DE USUARIOS Y SEGURIDAD INFORMATICA"** en el que plasma un conjunto de disposiciones del buen uso de la infraestructura informática.

Que, con **Informe N°757-2023-MDE/GRH** el Gerente de Recursos Humanos Abog. **VICTOR MELENDEZ GARCIA,** de fecha 27 de abril del 2023 en su análisis determinan: (...) *lo propuesto por la Sub Gerencia de Informática y Sistemas se encuentra enmarcado dentro de los presupuestos señalados por el RIS.*

Que la Sub Gerencia de Informática y Sistemas - MDE, en el marco de obtener un buen funcionamiento delas aplicaciones informáticas y de todos los equipos de cómputo por parte de los funcionarios y servidores de la Municipalidad Distrital de La Esperanza, proponen el proyecto de la directiva interna, denominada: **"DIRECTIVA DE USUARIOS Y SEGURIDAD INFORMATICA"**

Que, el Proyecto de Directiva: **"DIRECTIVA DE USUARIOS Y SEGURIDAD INFORMATICA",** se encuentra alineada a la Ley Orgánica de Municipalidades y la normativa de la materia; por ello cuenta con la siguiente estructura:

- Objetivo
- Finalidad
- Base Legal
- Responsabilidades
- Disposiciones
- Correos Electrónicos
- Copias de Seguridad
- Supletoriedad
- Vigencia
- Definición de Términos

Que, la Directiva en mención, tiene como **Objetivo**, eestablecer lineamientos y procedimientos de carácter administrativo, técnico y operativo para la gestión y seguridad de la información que permita lograr los niveles de protección y control de acceso a los recursos informáticos dentro de la Municipalidad Distrital de la Esperanza.

MUNICIPALIDAD DISTRITAL DE LA ESPERANZA

CREADO EL 29 DE ENERO DE 1965 - LEY N° 15418

Jr. Carlos María de Alvear N° 999 - Teléfonos: 272478 - 483330 - 272345 - 271744

TRUJILLO - PERÚ

RESOLUCION DE ALCALDIA N° 0575-2023-MDE

Que, el **Articulo VIII del Título Preliminar de la Ley Nº 27972, Ley Orgánica de Municipalidades:** *"Los gobiernos locales están sujetos a las leyes y disposiciones que, de manera general y de conformidad con la Constitución Política del Perú, regulan las actividades y funcionamiento del Sector Público; así como a las normas técnicas referidas a los servicios y bienes públicos, y a los sistemas administrativos del Estado que por su naturaleza son de observancia y cumplimiento obligatorio. Las competencias y funciones específicas municipales se cumplen en armonía con las políticas y planes nacionales, regionales y locales de desarrollo"* concordante con lo **prescrito en el inciso 6) Artículo 20° del mismo cuerpo normativo. - atribuciones del alcalde**: *"dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas".*

Que, estando a lo expuesto, y de conformidad con lo prescrito en la Ley Orgánica de Municipalidades – Ley N°. 27972 y a las facultades y atribuciones establecidas en la misma;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR la **DIRECTIVA N° 03-2023-MDE-"DIRECTIVA DE USUARIOS Y SEGURIDAD INFORMATICA,** en mérito al **Informe N°757-2023-MDE/GRH.**

ARTÍCULO SEGUNDO.- NOTIFICAR el presente acto resolutivo a Gerencia Municipal, Sub Gerencia de Informática y Sistemas y demás áreas competentes, para su conocimiento y fines pertinentes.

REGISTRESE, COMUNIQUESE Y ARCHIVESE

YSR/OLSS
M
GlyS
CI
PORTAL INSTITUCIONAL

MUNICIPALIDAD DISTRITAL DE LA ESPERANZA

Wilmer Sánchez Ruiz
ALCALDE

MUNICIPALIDAD DISTRITAL DE LA ESPERANZA

SUBGERENCIA DE INFORMATICA Y SISTEMAS

DIRECTIVA N° 003-2023-MDE

Aprobada con R.A. N° 0575-2023-MDE

"LINEAMIENTOS Y PROCEDIMIENTOS DE CARÁCTER ADMINISTRATIVO, TÉCNICO Y OPERATIVO PARA LA GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN"

1. OBJETIVO:

El presente documento establece los lineamientos y procedimientos de carácter administrativo, técnico y operativo para la gestión y seguridad de la información que permita lograr los niveles de protección y control de acceso a los recursos informáticos dentro de la Municipalidad Distrital de La Esperanza.

2. FINALIDAD:

Optimizar la gestión municipal, a fin de preservar la integridad de los recursos informáticos y cautelar el correcto uso de los equipos de cómputo, conectividad en redes, componentes informáticos, sistemas operativos y software en la Municipalidad Distrital de La Esperanza.

3. ALCANCE:

La presente Directiva es de obligatorio cumplimiento y aplicación de todos los trabajadores de la Municipalidad Distrital de La Esperanza. Incluye practicantes, voluntariado y locador de servicios.

4. BASE LEGAL:

- Norma Técnica Peruana-ISO/IEC 27001:2014.
- Directiva Nº 010-2002-INEI/DTNP.
- Ley N° 29733, Ley de Protección de Datos Personales
- Decreto Legislativo N° 822, Protección Jurídica del Software – Ley del derecho de autor.

5. RESPONSABILIDADES:

a) El seguimiento al cumplimiento de la presente Directiva, así como cualquier consulta o aclaración por parte de los usuarios le corresponde a la Subgerencia de Informática y Sistemas.

b) La Subgerencia de Informática y Sistemas deberá supervisar el cumplimiento de la presente Directiva, la misma que será revisada anualmente, con la finalidad de realizar mejoras, de ser necesario.

c) La presente Directiva deberá ser difundida por la Gerencia Municipal o a quien se designe, para conocimiento de todo el personal de la Municipalidad Distrital de La Esperanza.

d) Todo el personal de la Municipalidad Distrital de La Esperanza deberá cumplir con lo dispuesto en la presente Directiva. El incumplimiento a la presente Directiva será comunicado formalmente, mediante informe, por parte de la Subgerencia de Informática y Sistemas al titular del órgano o unidad orgánica del usuario responsable de dicho incumplimiento, a la Gerencia de Recursos Humanos y a la Gerencia Municipal. Se aplicará el Reglamento Interno de Trabajo y de otras normas que le fuera aplicable según corresponda.

e) Los órganos y unidades orgánicas son responsables de comunicar a la Subgerencia de Informática y Sistemas cualquier situación que advierta respecto al incumplimiento de la presente Directiva.

6. DISPOSICIONES:

6.1. USO DE LOS RECURSOS INFORMÁTICOS:

Los recursos informáticos de la MDE están conformados por todo el equipamiento de hardware (computadoras, servidores, impresoras, escáneres, etc.) y software, sean éstos de terceros, herramientas de internet o desarrollados dentro de la MDE, así como los equipos de comunicación (módem, router, switch, etc.), también lo conforman los medios que permiten la transferencia de datos (cables, antenas, etc.). Al respecto:

a) La instalación y configuración de los recursos informáticos es responsabilidad del personal de la Subgerencia de Informática y Sistemas; cualquier cambio a la configuración de algún equipo debe ser autorizado y ejecutado por el personal expresamente autorizado.

b) Ningún usuario debe dañar deliberadamente los recursos informáticos de la MDE, tampoco degradar o detener su operatividad (performance), ni privar de acceso a personal autorizado a estos recursos.

c) Es responsabilidad del usuario final la eficacia de las medidas de control sobre los recursos informáticos, para lo cual deberá seguir las pautas puestas a su disposición en esta Directiva.

6.2. DE LAS ESTACIONES DE TRABAJO (Personal Administrativo):

a) Los equipos de cómputo son de uso exclusivo para las labores que han sido asignadas a cada trabajador. Estos no deben ser usados para fines personales o actividades no relacionadas a la MDE. Cada usuario es responsable del buen uso de los equipos de cómputo asignados.

b) Los usuarios son responsables de bloquear sus respectivos equipos de cómputo (PC) cuando se ausenten momentáneamente de su puesto de trabajo; para ello deben pulsar las teclas "CTRL", "ALT" y "SUPR" o "DEL" en algunos casos y luego seleccionar la opción "Bloquear". Esto impide tanto el acceso no autorizado al equipo de cómputo, como a las aplicaciones. El usuario que no deje bloqueado su computador al ausentarse será responsable por el uso no autorizado del equipo, de la red o de las aplicaciones instaladas.

c) Queda terminantemente prohibido guardar en los discos duros de las computadoras de la MDE archivos de música y video, cuando estos no sean utilizados en sus actividades laborales y funciones asignadas.

d) Está autorizado a los usuarios finales compartir archivos o carpetas que contenga información de índole laboral a través de la red local.

e) Está prohibido para los usuarios finales compartir archivos o carpetas que no contenga información de índole laboral, pues esta práctica pone en riesgo el rendimiento de la red institucional. La Subgerencia de Informática y Sistemas, está facultada a tomar las medidas preventivas y correctivas necesarias.

f) La ubicación actual del usuario y de su estación de trabajo forman parte de la implementación de cableado estructurado de red; por ello, todo cambio de ubicación debe darse en coordinación con la Subgerencia de Informática y para la determinación de la factibilidad técnica de los trabajos de acondicionamiento del cableado estructurado de red de datos; solo de esta manera se garantiza la conexión a la red de la estación de trabajo del usuario.

g) Todos los usuarios cuentan con un control de acceso al Sistema Operativo para evitar accesos no autorizados a las computadoras. El acceso solo se podrá realizar mediante la autenticación del usuario.

h) Se debe contar con un control para la identificación y autenticación único y exclusivo para uso personal, a fin de manifestarse y auditarse las actividades de cada responsable particular.

i) El uso de la red local de datos para equipos de cómputo de terceros (no institucionales) para fines institucionales, que requieran internet u otro servicio, deberá ser autorizado por escrito por la Gerencia Municipal o nivel superior.

6.3. USO DE SOFTWARE:

La copia de software de propiedad de la MDE; salvo que la copia del software sea para fines de respaldo y sólo en caso de estar permitido por la licencia del software.

La Subgerencia de Informática y Sistemas tiene como responsabilidad establecer mecanismos de restricción de acceso por perfiles para:

- La instalación de software no autorizado.
- Acceso a opciones de configuración de los computadores.

La instalación de software sin licencia en una PC debe ser autorizado por la Gerencia Municipal. Si la MDE cuenta con la licencia de software respectiva disponible, se procederá con la instalación; el software debe ser instalado únicamente por el personal de la Subgerencia de Informática y Sistemas.

6.4. DEL CONTROL DE ACCESOS:

La Subgerencia de Informática y Sistemas genera la cuenta de usuario a cada trabajador, así como también su contraseña.

La creación de una cuenta de usuario de acceso al dominio interno de la MDE es factible para el personal de la MDE al momento de adquirir vínculo laboral con la misma desde el inicio de sus actividades y/o cuando lo solicite el jefe inmediato superior o cuando exista un documento de designación.

La gestión de acceso de usuarios evita accesos no autorizados (a los sistemas de información, servicios, así como a las redes). Esto contempla la supervisión de los accesos.

Todo usuario tiene una cuenta que lo identifica. Cada cuenta de usuario es específica y debe cumplir con la siguiente política de conformación y sintaxis:

- Primera letra nombre del usuario, seguido del primer apellido.
- En caso de existir una cuenta de usuario de dominio coincidente con la que se pretende crear, se añadirán progresivamente las letras del segundo nombre del usuario hasta conseguir evitar la coincidencia con la nueva cuenta de usuario de dominio.

Para acceder al Sistema Operativo se cuenta con controladores de Dominio que autentican a los usuarios cuando éstos inician una sesión e ingresan a la red de la MDE.

La conexión será validada sólo si el usuario ha ingresado todos los datos solicitados: usuario y contraseña y se registra en el visor de eventos de los Controladores de Dominio su intento de ingreso sea éste exitoso o no.

La Subgerencia de Informática y Sistemas desactivará las cuentas de usuario de los trabajadores, y se realizará de acuerdo a los siguientes casos:

- Culminación de contrato.
- Cese o jubilación del trabajador.
- Vacaciones.
- Suspensión temporal de actividades laborales.
- Suspensión definitiva.
- Cambio de área.
- Otros que considere conveniente la Subgerencia de Informática y Sistemas.

Para los casos descritos en el párrafo anterior, la Gerencia de Recursos Humanos informará por escrito a la Subgerencia de Informática y Sistemas, respecto a la

situación laboral en que se encuentre el trabajador, teniendo en cuenta lo planteado, bajo responsabilidad de la Gerencia de Recursos Humanos.

Para la activación de la cuenta de usuario, el jefe inmediato superior lo solicitará a la Subgerencia de Informática y Sistemas. En caso de gerentes, subgerentes y jefes de área, la solicitud será en forma personal.

El acceso a los servicios restringidos de la red (streaming Ej. Youtube), redes sociales (Ej. Facebook), etc.) deberá ser solicitado por el jefe inmediato superior, del área usuaria, al que pertenece el usuario y estará sujeto a la aprobación de la autoridad correspondiente.

Se autoriza el acceso remoto exclusivamente para labores de administración de sistemas, aplicaciones y servicios críticos de la MDE, únicamente a usuarios autorizados de la Subgerencia de Informática y Sistemas.

6.5. DE LAS CONTRASEÑAS Y SEGURIDAD:

Las contraseñas representan un factor fundamental de la seguridad de los recursos informáticos, ya que es la primera línea de protección para el usuario y para la red.

a) La contraseña es asignada al usuario al momento de activar cada cuenta.
b) Al inicio de la sesión del sistema operativo, cada usuario está obligado a cambiar la contraseña que le fue asignada por la Subgerencia de Informática y Sistemas.
c) Para garantizar la confidencialidad de la información en la red de la MDE el formato y sintaxis de cada contraseña queda establecido bajo los siguientes lineamientos:
    - No puede tener menos de 6 caracteres (puede ser de 6 o más caracteres).
    - Puede ser una combinación con números y letras.
    - Vigencia de noventa (90) días calendarios, al término de los cuales el Sistema de Seguridad solicitará automáticamente al usuario el cambio de contraseña, no pudiendo repetir las dos últimas. Esta política aplica a todos los usuarios, con excepción de la Subgerencia de Informática y Sistemas.
    - Se recomienda cambiar las contraseñas con mayor frecuencia o cuando el usuario sospeche que la seguridad de su contraseña puede estar comprometida o vulnerada.
    - Las contraseñas no deben ser palabras comunes o simples.
    - No usar el nombre del trabajador, nombre de la computadora, servidor o nombre de alguna empresa.
d) Las contraseñas no deben ser enviadas en mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica. Tampoco deben ser reveladas o escritas en notas, documentos u otros medios escritos, incluyendo conversaciones telefónicas.

A partir de la activación de la cuenta de usuario y establecimiento de la contraseña, el usuario asume la responsabilidad sobre la inviolabilidad de esta. El propietario de una cuenta de usuario es el único responsable del uso que se le dé a ésta. Siendo la cuenta de usuario y su contraseña, de carácter personal e intransferible, queda totalmente prohibido compartirlas para ser usados por otras personas. Por lo mismo, está prohibido solicitar el reinicio de la contraseña de una cuenta de dominio para ser utilizada por personal distinto a su titular, sin importar el sustento (enfermedad repentina, ausencia al trabajo, vacaciones, etc.).

Si el usuario detecta que su cuenta ha sido vulnerada deberá de informar inmediatamente a la Subgerencia de Informática y Sistemas para que se ejecute las acciones correspondientes a este hecho.

Ante situaciones de sustracción o pérdida de información causados por la violación de la cuenta de usuario, debido a una definición débil de su contraseña o un mal uso de la misma, el usuario será responsable por los daños que pueda causar a los recursos informáticos de la MDE, los cuales serán evaluados por la Subgerencia de Informática y Sistemas, y luego comunicados a la Gerencia Municipal y/o Gerencia de Recursos Humanos para su evaluación y sanción que corresponda.

6.6. DE LOS CENTROS DE DATOS – DATA CENTER:

Para su acceso físico se ha establecido lo siguiente:

a) Las áreas y el entorno donde se encuentran el Data Center, deben ser un área segura, controles de entrada y acceso apropiados para prevenir la exposición a riesgo de sabotaje, robo de información y de los recursos de tratamiento de información y evitar pérdidas, daños o comprometer la actividad y continuidad del servicio.

b) Los equipos y servidores de la infraestructura informática de la MDE están ubicados en el Data Center del local del Palacio Municipal de la MDE.

c) Queda estrictamente prohibido el acceso al personal que no labora en la Subgerencia de Informática y Sistema, salvo autorización expresa.

6.7. DE LOS EQUIPOS DE COMUNICACIÓN:

Se refiere a los equipos de comunicación de la infraestructura de comunicaciones de la MDE, que se encuentran instalados en los diferentes locales.

Se deben establecer medidas de seguridad para la administración de los equipos de comunicaciones, tales como clave de acceso, servicio de alimentación ininterrumpida, flujo de alimentación estabilizada, sistema de refrigeración, así como control del acceso solo a personal autorizado.

a) Queda prohibido el acceso y la manipulación a dichos equipos por otro personal que no sea de la Subgerencia de Informática y Sistemas.

b) Los equipos de comunicación deben estar protegidos dentro de un gabinete cerrado con llave.

c) Es responsabilidad de la Subgerencia de Informática y Sistemas, llevar un inventario de todos los recursos de comunicación, en donde se registra la ubicación, modelo, fin, detalles propios como: serie, código patrimonial, etc. Todo traslado, manipulación y/o modificación de las configuraciones deben ser autorizados por el área indicada a fin garantizar el normal desenvolvimiento de las actividades.

6.8. PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS Y MALWARE:

La Subgerencia de Informática y sistemas, es responsable de implementar una solución antivirus, que reduzca la probabilidad de una infección directa en las computadoras.

a) Cuando se detecte una infección o ataque en progreso, originado por el uso de medios extraíbles de almacenamiento, el usuario será responsable por los daños de software y/o hardware causados por dicha infección, por lo cual los usuarios deberán tener mucho cuidado en que los dispositivos que traigan no hayan sido utilizados en otras computadoras infectadas.

b) Queda terminantemente prohibido a los usuarios finales la descarga de archivos y/o programas (software gratuito). En caso se requiera algún programa del tipo gratuito, deberá ser solicitado a la Subgerencia de Informática y Sistemas, especificando el motivo de la necesidad y en que computadora(s) será(n)

instalada(s). Previa evaluación de riesgos, dicho requerimiento será evaluado antes de ser atendido.

c) Se debe contar con una solución de Filtro de Contenido web, para restringir la navegación por páginas web prohibidas y para mitigar la infección por descarga de archivos y software de internet.

Si en un computador se detecta una infección o malware en progreso o propagación, el personal de la Subgerencia de Informática y Sistemas, está facultado a tomar el control físico o remoto del equipo de cómputo en cuestión, a fin de controlar y mitigar los efectos del agente dañino.

7. CORREOS ELECTRONICOS:

a) La estructura del nombre de la cuenta de correo electrónico institucional para cada usuario estará formada por la primera letra del primer nombre del usuario seguido del apellido paterno, ligado con el símbolo @ al nombre de dominio (@muniesperanza.gob.pe) de la Institución (establecido por la Directiva N°010-2002-INEI/DTNP "Normas Técnicas para la Asignación de Nombres de Dominio de las entidades de la Administración Pública").

b) En caso de existir dos construcciones similares, el administrador de correo electrónico adicionará la primera letra del apellido materno. De continuar la coincidencia, se completarán más letras del segundo apellido.

c) La asignación de las cuentas de correo se atenderá conforme al número de cuentas con que cuenta la entidad.

d) La cuenta de correo electrónico es personal, intransferible e irrenunciable, asimismo, al tener una cuenta de correo electrónico institucional se compromete y obliga a cada usuario a aceptar las normas establecidas por la Ley, la normativa vigente sobre la materia y las establecidas por la Institución. así como, a someterse a ellas.

e) El usuario solo podrá usar el correo institucional mientras esté vinculado con la institución.

f) La Gerencia de Recursos Humanos deberá informar por escrito a la Subgerencia de Informática y Sistemas,

g) Ningún usuario está facultado a usar otro correo electrónico que no sea el correo institucional para comunicación oficial de la MDE.

h) El trabajador debe leer, de manera obligatoria, su correo electrónico durante su permanencia en la institución. Por este motivo debe mantener en línea el cliente de correo electrónico que utilicen.

i) En caso de recibir mensajes de procedencia desconocida y con archivos adjuntos debe reportarlo a la Subgerencia de Informática y Sistemas a fin de proceder a eliminar dicho correo. Bajo ningún motivo el usuario deberá abrir el mensaje o su contenido adjunto.

8. COPIAS DE SEGURIDAD – BACKUP:

Es de responsabilidad de cada trabajador solicitar a la Subgerencia de Informática y Sistemas, que se realice una copia de seguridad - Backup de la información (archivos digitales) del área que se encuentran almacenados en el equipo de cómputo que se indique.

El Backup, debe almacenarse en el disco duro del mismo equipo de cómputo o en algún medio magnético y, deberá quedar bajo custodia del trabajador usuario del equipo de cómputo y/o responsable del área al cual pertenece.

9. SUPLETORIEDAD:

Los casos no tipificados en la presente directiva, respecto al mal uso de la Tecnología de la Información, se rigen supletoriamente con lo establecido por otras normas de ámbito nacional.

10. VIGENCIA:

Entrará en vigor a partir de su aprobación mediante Resolución Administrativa o Acuerdo de Concejo.

11. DEFINICIÓN DE TÉRMINOS:

Confidencialidad: Principio fundamental de seguridad que busca garantizar que toda la información de los trabajadores, y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

Disponibilidad: Principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando está es requerida por el proceso del negocio. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento.

Estación de Trabajo: Área destinada para que un usuario de la red pueda acceder a la misma mediante dispositivos de red (Pc's, Laptop, tablet, etc.).

Firewall: Normalmente conocido como barrera cortafuegos. Es un filtro en software o hardware que controla todas las comunicaciones entrantes y salientes de una red a otra red, cuya función principal es denegar o permitir el acceso de dicha comunicación. Así para denegar o autorizar una comunicación, el firewall primero analiza el perfil del usuario si tiene o no acceso a un determinado servicio tales como: acceso a Internet, correo, transferencia FTP, etc.; y luego denegará o dará paso a dicha comunicación.

Integridad: Principio fundamental de seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas de la organización, así como evitar fraudes y/o irregularidades de cualquier índole que haga que la información no corresponda a la realidad.

LAN (Local Área Network): Red de Área Local, tipo de arreglo para comunicación de datos a alta velocidad (típicamente en el rango de los Mbit/s) en donde todos los segmentos del medio de transmisión (cable de par trenzados, o fibras ópticas) están circunscritos a una región geográficamente reducida.

Malware: Se define como software malicioso que cubre un amplio rango de software hostil como son los virus, gusanos, caballos de troya, etc., capaces de causar daños o alteraciones del sistema operativo, archivos, u otros componentes de computadoras y redes informáticas.

Memoria USB (Universal Serial Bus): Dispositivo de almacenamiento que utiliza una memoria flash para guardar información.

Seguridad de la Información: Conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software.

Soporte Técnico: Servicio de soporte en línea que brinda la Subgerencia de Informática y Sistemas a todos usuarios de la MDE. Cuenta con herramientas en hardware y software que le permite colaborar en la resolución de cualquier tipo de problemas.

SPAM: Se define como Correo Electrónico "tipo basura" o también conocido como "correo no solicitado". Estos mensajes son normalmente enviados a través de listas de correo invisibles o grupos de noticias que bombardean con propaganda de todo tipo de productos o servicios. Muchos de estos mensajes vienen infectados de virus, gusanos y caballos de Troya.

Spyware: Software parásito que actúa como espía o secuestrador, y se auto instala en un computador sin el permiso del usuario. Así existen varios tipos de spyware, unos que recopilan y sustraen información para luego enviarla a una institución externa, otros actúan como secuestradores de las herramientas de navegación. Su funcionamiento puede traer serios problemas de estabilidad y rendimiento en la computadora infectada, llegando incluso a inhibir la misma. Normalmente causan serias dificultades a la hora de conectarse a Internet.

Virus: Pequeño programa malicioso, escrito intencionalmente para auto instalarse en la computadora de un usuario sin conocimiento o permiso de éste. Se comporta como un programa parásito porque infecta y ataca a los archivos contenidos en el computador. Para propagarse, se replica a sí mismo ilimitadas veces, llegando a producir serios daños que pueden afectar a los sistemas y archivos en general, pudiendo estos últimos daños borrar, corromper o destruir dichos archivos.