EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

AEFCIUDAD MÉXICO
AUTORIDAD EDUCATIVA FEDERAL EN LA CIUDAD DE MÉXICO

DIRECCIÓN GENERAL DE PLANEACIÓN, PROGRAMACIÓN Y EVALUACIÓN EDUCATIVA

CENTRO DE DESARROLLO INFORMÁTICO ARTURO ROSENBLUETH

GUÍA PARA EL USO DE EQUIPOS DEL "SERVICIO DE ARRENDAMIENTO DE CÓMPUTO (SAC) EN LA AUTORIDAD EDUCATIVA FEDERAL EN LA CIUDAD DE MÉXICO".

FEBRERO 2021

ÍNDICE

1. OBJETIVO.

Establecer los criterios, acciones y alcances de las responsabilidades en materia de Tecnología de la Información y Comunicaciones (TIC) para el uso de Equipo de Cómputo que apliquen a los servidores públicos de los Centros de Trabajo Educativos y Administrativos de la Autoridad Educativa Federal en la Ciudad de México (AEFCM), asegurando óptimas condiciones en la operación, control, recepción, configuración, ubicación y manejo de los equipos de cómputo.

2. FUNDAMENTO LEGAL.

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Orgánica de la Administración Pública Federal.
- Ley General de Educación.
- Ley General del Sistema Nacional Anticorrupción.
- Ley General de Responsabilidades Administrativas.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Ley Federal de Austeridad Republicana.
- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- Reglamento Interior de la Secretaría de Educación Pública.
- Decreto por el que se reforma el diverso por el que se crea a Administración Federal de Servicios Educativos en el Distrito Federal, como un órgano administrativo desconcentrado de la Secretaría de Educación Pública.
- Manual de Organización General de la Autoridad Educativa Federal en la Ciudad de México.
- Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

- Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información (MAAGTICSI).

- Lineamientos por los que se establecen medidas de austeridad en el gasto de operación en las dependencias y entidades de la Administración Pública Federal.

3. ÁMBITO DE APLICACIÓN.

La presente Guía es de observancia obligatoria para todos los servidores públicos de los Centros de Trabajo Educativos y Administrativos de la Autoridad Educativa Federal en la Ciudad de México (AEFCM) que cuenten con Equipo de Cómputo de escritorio o móvil, incluyendo sus componentes.

La Unidad responsable de proveer de infraestructura y servicios de Tecnologías de Información y Comunicaciones a las demás áreas y unidades administrativas de la AEFCM es el **Centro de Desarrollo Informático "Arturo Rosenblueth".**

Derivado de lo anterior se emiten la siguiente **Guía para el uso de Equipos del "Servicio de Arrendamiento de Cómputo (SAC) en la Autoridad Educativa Federal en la Ciudad de México".**

4. DISPOSICIONES.

I. DE LAS OBLIGACIONES DE LOS USUARIOS.

Es responsabilidad de los usuarios de la AEFCM que cuenten con Equipos de Cómputo de escritorio o móvil, incluyendo sus componentes, cumplir con la siguiente **Guía para el uso de Equipos del "Servicio de Arrendamiento de Cómputo (SAC) en la Autoridad Educativa Federal en la Ciudad de México"**.

- **Resguardo.**

El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones de la AEFCM.

El usuario es responsable del cuidado de los equipos asignados y sus componentes integrados para el equipo de cómputo de escritorio: el CPU, monitor, teclado y mouse. Para el equipo de cómputo personal móvil o portátil, también llamado laptop; mouse y maletín. Quedando de conformidad que

a la firma del documento correspondiente quedan bajo su resguardo, así como de la información y contenido que estén almacenados y procesados en dichos equipos.

- **Protección del Equipo Informático.**

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

El usuario deberá reportar de forma inmediata, tanto a la Coordinación Administrativa o en su caso al Enlace Administrativo de su área, como a la Dirección de Infraestructura del Centro de Desarrollo Informático "Arturo Rosenblueth" (CDIAR); cuando detecte que existen riesgos ambientales que puedan afectar a los equipos de cómputo, como pueden ser fugas de agua, conatos de incendio u otros.

Es responsabilidad del usuario, evitar en todo momento la fuga de información de la AEFCM que se encuentre almacenada en los equipos de cómputo, que tenga asignado.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor y del CPU, así como mantener el equipo informático en un entorno limpio y sin humedad.

- **Componentes originales**.

Es obligación del usuario mantener el equipo de cómputo con sus componentes originales.

- **Reubicación de los equipos**.

Los usuarios no deben mover, reubicar o desarmar los equipos de cómputo, instalar o desinstalar dispositivos, ni retirar sellos de éstos sin la autorización previa. En caso de requerir este servicio deberá ser solicitado con anterioridad a la Dirección de Infraestructura del CDIAR.

Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de una reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Dirección de Infraestructura del CDIAR, a través de un plan detallado de movimientos debidamente autorizados por el Director del Área que corresponda.

- **Pérdida de Equipo.**

El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia durante el horario de labores; en consecuencia, responderá por dicho bien de acuerdo con la normatividad vigente en los casos de robo, extravío o pérdida de este.

El resguardo para la laptop tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

En caso de la desaparición, robo o extravío del equipo de cómputo, laptop o accesorios bajo su resguardo, el usuario aplicará el procedimiento indicado en el apartado de **INCIDENCIAS.**

- **Uso de dispositivos especiales.**

Si alguna área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por la Dirección de Infraestructura del CDIAR.

- **Entrada de los equipos de cómputo y componentes a las instalaciones de la AEFCM.**

Cualquier persona que tenga acceso a las instalaciones de la AEFCM, deberá registrar al momento de su entrada, el equipo de cómputo, laptop, medios de almacenamiento y herramientas que no sean propiedad de la AEFCM, el cual, podrá retirar el mismo día.

- **Daño del equipo.**

El equipo de cómputo o laptop que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso, la Dirección de Infraestructura del CDIAR determinará la causa de dicha descompostura.

- **Instalación de software.**

Los usuarios que requieran la instalación de software adicional al precargado, deberán justificar el uso y solicitar la autorización a la Dirección de Infraestructura del CDIAR a través de un oficio firmado por su Dirección de adscripción, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación, mostrando su respectiva licencia de uso.

- **Configuración**.

Los usuarios de las áreas de la AEFCM, no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo, utilizando el protocolo de transferencia de archivos (FTP) u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la AEFCM, sin la autorización de la Dirección de Infraestructura del CDIAR.

- **Seguridad para la red.**

Será considerado como un ataque a la Seguridad de la Información y una falta grave, cualquier actividad no autorizada por la Dirección de Infraestructura del CDIAR, mediante equipos de cómputo donde los usuarios realicen la exploración de la red de la AEFCM, así como de las aplicaciones que sobre dicha red operan, con fines de detectar una posible vulnerabilidad.

- **Controles contra código malicioso**.

Los usuarios de la AEFCM que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso (Vacunar dispositivos USB, Discos Externos, etc.), como puede ser virus o malware.

Para prevenir infecciones por virus informático, los usuarios de la AEFCM no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Dirección de Infraestructura del CDIAR.

Los usuarios de la AEFCM deben verificar que la información y los medios de almacenamiento, considerando al menos discos externos y USB, estén libres de cualquier tipo de código malicioso, para lo cual, deben ejecutar el software antivirus autorizado por la Dirección de Infraestructura del CDIAR.

Para todos los archivos de computadora que sean proporcionados por personal externo o interno, considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario deberá verificar que estén libres de virus utilizando el software antivirus autorizado por la Dirección de Infraestructura del CDIAR antes de ejecutarse.

Ningún usuario de la AEFCM debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para autoreplicarse, dañar, o en otros casos, impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software, mucho menos probarlos en cualquiera de los ambientes o plataformas de la AEFCM. El incumplimiento de esto será considerado una falta grave.

Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico y de mensajería instantánea. Así como acceder a redes de comunicaciones externas, sin la debida autorización de la Dirección de Infraestructura del CDIAR.

Cualquier usuario que sospeche de alguna infección por virus informático, dejará de usar inmediatamente el equipo y llamar la Dirección de Infraestructura del CDIAR para la detección y erradicación del virus.

Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal o móvil será responsable de solicitar a la Dirección de Infraestructura CDIAR periódicamente las actualizaciones del software antivirus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y prevenir la propagación de virus. Debido a que algunos virus son extremadamente complejos, ningún usuario de la AEFCM debe intentar erradicarlos de las computadoras personales o móviles.

- **Internet.**

El acceso a Internet provisto a los usuarios de la AEFCM, es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeñan.

La asignación del servicio de Internet se solicitará por escrito mediante correo electrónico a la Dirección de Infraestructura del CDIAR, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Director de Área correspondiente.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el AEFCM.

Los usuarios de Internet de la AEFCM, tienen que reportar todos los incidentes de Seguridad de la Información a la Dirección de Infraestructura del CDIAR, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de Seguridad de la Información.

Los usuarios de navegación en Internet, al aceptar dicho servicio, están accediendo a ser sujetos de monitoreo de actividades que realizan en Internet y detección de sitios web que no tengan ninguna relación con la labor que se desempeña en su horario de trabajo, a continuación, se enlistan algunos sitios prohibidos:

- Sitios Web de Juegos.
- Sitios Web de Apuestas.
- Sitios Web de Contenido de Adultos.
- Sitios Web de descargas de archivos maliciosos.
- Sitios Web de Videos.
- Sitios Web de Música.

Además, los usuarios saben en particular lo siguiente:

- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización de la Dirección de Infraestructura del CDIAR.
- Saben que la utilización de Internet es para el desempeño de su función y puesto en la AEFCM y no para propósitos personales.
- Saben que deben cumplir con lo establecido en este documento.

- **Controles de acceso.**

Los usuarios deberán mantener sus equipos de cómputo personal y móvil con controles de acceso como password, protectores de pantalla (screensaver) e imagen en el escritorio previamente autorizados e instalados por la Dirección de Infraestructura del CDIAR.

La asignación del password debe ser realizada de forma individual, por lo que el uso de passwords compartidos está prohibido.

Cuando un usuario olvide, bloquee o extravíe su password, deberá levantar un reporte a la mesa de ayuda del CDIAR para que se le proporcione un nuevo password y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a su equipo de cómputo.

Está prohibido que los passwords se encuentren de forma legible en cualquier medio impreso o dejarlos en un lugar donde personas no autorizadas puedan encontrarlos.

Sin importar las circunstancias, los passwords nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su password de todas las acciones que se realicen con el mismo.

Todos los usuarios deberán observar lo siguiente para la construcción de sus passwords:

Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10), estos caracteres deben ser alfanuméricos.

Deben ser difíciles de adivinar, esto implica que los passwords no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen número o listas secuenciales.

No deben ser idénticos o similares a passwords que hayan usado previamente.

Todo usuario que tenga la sospecha de que su password es conocido por otra persona, deberá cambiarlo inmediatamente.

Los usuarios no deben almacenar los passwords en ningún programa o sistema que proporcione esta facilidad.

Los cambios o desbloqueo de passwords solicitados por el usuario a la Dirección de Infraestructura del Centro de Desarrollo Informático "Arturo Rosenblueth" (CDIAR) serán notificados con posterioridad por correo electrónico al solicitante con copia a su Dirección correspondiente, de tal forma que se pueda detectar y reportar cualquier cambio no solicitado.

- **Cambio de Equipo de Cómputo.**

El usuario deberá definir y preparar la información que se va a respaldar incluyendo todos sus archivos y carpetas de trabajo.

El respaldo de la información del usuario (archivos con extensiones *.DOC, *.XLS, *.PPT, *.PDF, entre otros) **será responsabilidad del usuario** y los archivos del equipo (archivos con extensiones .PST, .PAB, .MSG, entre otros) será realizado por el proveedor de acuerdo a lo que indique el usuario y por ningún motivo podrán ser respaldados archivos con extensiones: avi, mpg, mov, mpeg, dvm, fli, flc, asf, real, swf, asx, mp3, mid, wav, ra, y jpg.

El usuario será el responsable de verificar que toda la información y los archivos estén contenidos en el equipo asignado.

El tiempo que lleve a cabo la asignación y configuración de una computadora de escritorio o móvil estará en función del volumen de datos, tipo de aplicaciones y servicios de información que contenga el equipo del usuario.

Antes de retirar el bien informático sujeto a reasignar o a dar de baja, el usuario deberá verificar que se le dé formato al disco duro del equipo que entrega. En caso del nuevo equipo asignado, deberá verificar el borrado de los archivos en el directorio temporal utilizado para restaurar la información.
Es responsabilidad del usuario a quien esté asignado el equipo de escritorio o portátil, la información contenida en la misma.

Cuando un usuario cambie de área, el equipo asignado a éste deberá permanecer dentro del área designada originalmente. Será responsabilidad de la nueva área en la que habrá de laborar el usuario, el proporcionarle el equipo de cómputo personal o móvil requerido para el desarrollo de sus funciones.

De acuerdo con los lineamientos de reducción de costos, optimización y eficiencia de los recursos, los bienes informáticos y periféricos de cómputo personal o móvil usados, podrán ser reciclados y asignados a un usuario antes de que éstos se vuelvan obsoletos.

- **Uso del Equipo**.

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

II. DE LAS OBLIGACIONES DE LAS COORDINACIONES ADMINISTRATIVAS.

- **Asignación de los Equipos de Cómputo**.

Todo empleado de la AEFCM de nuevo ingreso deberá de contar con una inducción sobre la **Guía para el uso de Equipos del "Servicio de Arrendamiento de Cómputo (SAC) en la Autoridad Educativa Federal en la Ciudad de México**".

En caso de alta, baja, cambio de resguardante o ubicación de cualquiera de los equipos relacionados con este servicio, deberán ser notificados a la Coordinación Administrativa (CA) o Área equivalente de cada Dirección General o Coordinación Sectorial de la AEFCM y a su vez, notificar por escrito al CDIAR y al Prestador de Servicios, de no ser así, el prestador de servicio no podrá dar trámite a las incidencias relacionadas con el servicio que se proporciona.

- **Resguardo de los Equipos de Cómputo.**

La Coordinación Administrativa o Enlace Administrativo, será la responsable de que los equipos de cómputo y sus componentes que el Prestador de servicios suministra como parte del servicio, se mantengan dentro del inmueble con el apoyo del personal de seguridad.

Al personal, visitantes o proveedores, se le registrará cualquier bolsa, mochila, portafolio o cualquier otro aditamento que pueda contener bienes informáticos que salgan de las instalaciones de la AEFCM con la finalidad de detectar la salida de bienes informáticos sin autorización.

Las computadoras personales, portátiles, y cualquier bien informático, podrá salir de las instalaciones de la AEFCM únicamente con la autorización de la Coordinación Administrativa o en su caso el Enlace Administrativo de su área.

Para el acceso de bienes informáticos y Accesorios, primero deberán registrarse con el personal de seguridad al ingresar a los inmuebles de la AEFCM.

- **Salida de los equipos de cómputo y/o componentes de las instalaciones de la AEFCM.**

Para la salida de más de 5 equipos de cómputo de las instalaciones de la AEFCM, que el Prestador de servicios suministra, corresponderá hacer de conocimiento a la Dirección de Infraestructura del CDIAR y deberá ser avalada por un pase de salida, expedido por su Coordinación Administrativa o en su caso el Enlace Administrativo de su área, en la que se considere los siguientes datos:

a) Fecha y hora de salida.
b) Destino del equipo.
c) Nombre y firma del funcionario que trasladará el equipo.
d) Nombre y firma del funcionario que autoriza la salida del equipo del inmueble.
e) Justificación o asunto de la salida del equipo y fecha de regreso del equipo al inmueble de la AEFCM de donde proviene el equipo.

En caso de encontrar algún bien informático o accesorio que no tenga autorización de salida de las instalaciones de la AEFCM, se deberá informar a la Coordinación Administrativa, o en su caso al Enlace Administrativo del área de cada Dirección General o Coordinación Sectorial de la AEFCM, lo anterior para verificar si el bien informático o accesorio en cuestión, es propiedad de la Institución o se encuentra en resguardo de la AEFCM, en caso de serlo, ésta será la responsable de ejecutar las acciones que determine pertinentes, de igual manera, en caso de que el bien informático o accesorio no sea propiedad, la Coordinación Administrativa o en su caso Enlace Administrativo, determinará las acciones pertinentes.

- **Inventario de los equipos.**

La Coordinación Administrativa o Área equivalente de cada Dirección General o Coordinación Sectorial de la AEFCM están obligadas a entregar un reporte general por lo menos cada 6 meses de altas, bajas o cambios del resguardante y ubicación de cualquiera de los equipos relacionados con este servicio, para mantener actualizada la información, indicando lo siguiente:

- En caso de ser un equipo de cómputo personal de escritorio en un Centro de Trabajo Escolar o Administrativo:

  - No. consecutivo
  - Clave de Centro de Trabajo (CCT)
  - Nombre del Centro de Trabajo
  - Nivel educativo
  - Turno
  - Domicilio de Centro de Trabajo (Calle, Núm., Colonia, C.P., Alcaldía)
  - Teléfono
  - Nombre completo del resguardante
  - Correo electrónico
  - Puesto del resguardante
  - No. Serie del CPU
  - No. serie del monitor
  - No. serie el UPS
  - Especificar Accesorios extras (Mouse, bocinas, entre otros)

- En caso de ser un equipo de cómputo móvil o Laptop de un Centro de Trabajo Administrativo:

  - No. consecutivo
  - Clave de Centro de Trabajo (CCT)
  - Nombre del Centro de Trabajo
  - Domicilio de Centro de Trabajo (Calle, Núm., Colonia, C.P., Alcaldía)
  - Teléfono

- Nombre completo del resguardante
- Correo electrónico
- Puesto del resguardante
- No. Serie de Laptop
- Especificar Accesorios extras (Mouse, bocinas, maletín, entre otros)

III. DE LAS OBLIGACIONES DE LA DIRECCIÓN DE INFRAESTRUCTURA.

- **Componentes Originales.**

Para intercambiar partes en los componentes de hardware y licencias de software del equipo asignado, se requiere previa aprobación por escrito de la Dirección de Infraestructura del CDIAR.

- **Mantenimiento de equipo**.

Únicamente el personal autorizado por la Dirección de Infraestructura del CDIAR podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

- **Administración de privilegios.**

Cada equipo de cómputo tiene habilitado tres tipos de perfiles; Usuario, Enlace y Universal/Administrador; de acuerdo con el cargo o encomienda, la Dirección de Infraestructura del CDIAR, lo habilitará.

A continuación, se definen los roles y responsabilidades para el servicio de cambio de equipo de cómputo personal o móvil[1]:

Actividad: R: Responde A: Apoyo	El proveedor	Enlace Informático	Usuario Final
Generación del respaldo de la información		A	R
Transferencia del respaldo de información del equipo a retirar	R		
Configuración de red conforme a la misma IP estática o direccionamiento dinámico DHCP del equipo a retirar, según sea el caso	R		
Restauración de información y configuraciones locales del equipo a habilitar	R	A	

[1] Apartado del anexo técnico denominado "Cambio de equipo de cómputo", del contrato plurianual AEFCM/004/DGPPEE/2018, celebrado con el proveedor "TED, Tecnología Editorial, S.A. de C.V.

Configuración de aplicaciones institucionales (aplicaciones legadas)		R	
Deshabilitación de la administración remota por *hardware* del equipo a retirar	R		
Actualización de la documentación de resguardos	R		

- **Movimientos de bienes informáticos de cómputo personal, periféricos.**

La Dirección de Infraestructura del CDIAR, deberá elaborar el pase de salida cuando algún bien informático de cómputo personal o móvil y periférico requiera ser trasladado fuera de las instalaciones de la AEFCM, por motivo de garantía o reparación.

- **Préstamo de equipo de cómputo, periféricos, software.**

No existe el préstamo de equipo de cómputo o móvil, periféricos, *software,* por lo que cada área usuaria deberá prever la solicitud de asignación de los recursos que necesite.

IV. DE LAS OBLIGACIONES DEL PROVEEDOR.

- **Resguardo de los servicios administrados.**

El proveedor de los bienes arrendados para uso de la AEFCM, será el responsable de dejar como evidencia un formato de resguardo de cada uno de los equipos, donde se señale el área y datos del usuario que operará, asimismo efectuará un acta de entrega que ampare la totalidad de los bienes entregados por sitio, de ambos documentos se deberá entregar el original a la Dirección de Infraestructura de la Coordinación Sectorial del Centro de Desarrollo Informático "Arturo Rosenblueth" de la AEFCM, y el proveedor podrá resguardar una copia de los mismos.

En el caso de que alguna Coordinación Administrativa o Enlace Administrativo, notifique algún cambio, deberá de actualizar los vales de resguardo correspondientes, así como el inventario de equipo de cómputo.

5. INCIDENCIAS.

Cuando ocurra una incidencia con un equipo y de los componentes, se deberá de notificar a la Coordinación Administrativa o Enlace Administrativo, con el reporte de servicio firmado por el usuario y el Prestador de servicios. En caso de que existiera alguna sustitución, esta deberá de generar un nuevo resguardo con los datos actualizados y conservar el historial de estos, así como enviar copia a la mesa de ayuda del SAC.

¿Qué hacer en caso de robo o siniestro?

1) **Levantar** Acta ante el Ministerio Público (MP).

2) **Realizar solicitud** al representante legal del Prestador de servicios mediante oficio sobre la reposición de los componentes sustraídos o faltantes.

3) Documentación en **ORIGINAL** para iniciar el trámite:

   a. Acta de hechos ante Ministerio Público (Robo).

   b. Acta de hechos de Protección Civil en caso de siniestro por fenómeno natural (Sismo, Inundación, Incendio, filtración de agua).

   c. Siniestro por daño físico:

      - Hablar a la mesa de servicios para levantar un número de Incidencia y solicitar la visita del técnico del prestador de servicio para su dictamen.

      - El técnico del prestador de servicio realizará su reporte señalando el daño del equipo y le informará al usuario el trámite a seguir por daño físico dejándole una copia de dicho reporte para gestionar la reposición y/o reparación del equipo.

4) Acta de Hechos para dar cumplimiento a los términos de la póliza de garantía, esta deberá contener lo siguiente:

   a. Clave del Centro de Trabajo (CCT).

   b. Nombre completo de la escuela o institución.

   c. Domicilio.

   d. Teléfono.

   e. Descripción completa del equipo.

      - Marca, Modelo y número de serie de cada equipo.

   f. Partes robadas.

   g. Nombre del responsable del equipo.

h. Hay que indicar que los equipos de cómputo son propiedad del prestador del servicio y no de la AEFCM, los cuales se encuentran en arrendamiento.

i. En el acta de hechos por siniestro y daño físico se debe integrar el reporte del técnico, donde emita su dictamen de valoración del equipo dañado.

5) Marcar copia del oficio de solicitud a la mesa de servicios del CDIAR que se dirigió al representante legal del Prestador de servicios, informando del incidente con anexos correspondientes, según sea el caso del incidente.

6) Correo electrónico para notificaciones a **mesadeayuda@aefcm.gob.mx.**

7) **Anexar Copia simple de la constancia de resguardo del equipo de cómputo** (documento entregado por el personal técnico de la empresa al ser instalado el equipo).

8) Enviar de manera inmediata la documentación a la Gerencia correspondiente del prestador del servicio considerando enviar copia a la Coordinación Administrativa o en Enlace, al CDIAR y a la mesa de ayuda del prestador del servicio en un plazo no mayor a 48 horas.

9) El prestador de servicio notificará mediante correo electrónico en un lapso no mayor a **72 horas al Área solicitante, así como, a la oficina de mesa de servicios del prestador del servicio,** si el acta cuenta con todos los requisitos necesarios para iniciar los trámites para la reposición, o de lo contrario señalará la información que haga falta para completar los datos en el acta y ésta pueda ser procedente.

10) El equipo de cómputo en cuestión, será repuesto en los siguientes 15 días hábiles a partir de la fecha de aceptación del Acta por parte del prestador del servicio.

Los equipos que ampara el resguardo se encuentran asegurados por el prestador del servicio, sin embargo, en caso de robo, extravío o siniestro (fenómeno natural o daño físico), el trámite requerido por el prestador del servicio para la recuperación de un componente será efectuado por el resguardante del equipo.

Todas las incidencias (fallas en la operación) relacionadas con los servicios antes señalados, deberán ser reportadas por el usuario afectado directamente a la mesa de servicios del prestador del servicio, al número telefónico y extensión asignados, así como al correo electrónico mesadeayuda@aefcm.gob.mx.

6. RESPONSABILIDADES.

- **Delitos en materia de TIC.**

En todos los actos cometidos por servidores públicos que se consideren violaciones graves como el robo, daño, modifique, destruya o provoque perdida de la información contenida en sistemas y equipos de informática, protegidos por algún sistema de seguridad, divulgue información reservada o confidencial de la AEFCM, se estará a lo dispuesto en el Título Noveno, Capítulo II relativo al Acceso Ilícito a Sistemas y Equipos de Informática, del Código Penal Federal.

En los casos en que el servidor público, omita en Registrar, Integrar, custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad, e impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos, se determinará lo procedente de acuerdo a lo establecido por los Títulos Tercero y Cuarto de la Ley General de Responsabilidades Administrativas.

Atendiendo a los actos u omisiones en que los Servidores Púbicos recaigan en presunta responsabilidad administrativa, penal o laboral, esta Unidad Administrativa dará vista al Órgano Interno de Control, así como a la Coordinación de Asuntos Jurídicos y Transparencia en la AEFCM, para que, en el ámbito de su competencia, realicen las acciones correspondientes tendientes a determinar la existencia de dicha responsabilidad.

7. DIRECTORIO DE SERVIDORES PÚBLICOS PARA DAR ATENCIÓN A EVENTUALIDADES.

CARGO	NOMBRE	TELÉFONO, EXTENSIÓN
Subdirector de Telecomunicaciones	Roberto Pérez López	55 3601-8799, ext. 43514
Director de Infraestructura	Eduardo Flores Mejía	55 3601-8799, ext. 43506

8. CONCEPTOS.

Para los efectos de la presente Guía, se entiende por:

Acceso Físico. Entrada o paso por donde se entra o se llega a un sitio dentro de la institución.

Acceso Lógico. Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo, o bien usar su información.

Acceso Remoto. Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.

Antivirus. Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o disquete.

Ataque. Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese activo y lograr afectarlo.

Archivo. Una colección identificada de registros relacionados.

Autorización. Es el proceso de asignar a los usuarios permisos para realizar actividades de acuerdo con su perfil o puesto.

Código Malicioso Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un caballo de Troya es ejemplo de un código malicioso.

Dispositivos especiales: Equipos no proporcionados por el proveedor (micrófonos, modem, router, antena, entre otros).

Falta administrativa Es falta administrativa todo acto u omisión del funcionario, intencional o culposo, que viole los deberes funcionales.

Freeware (Software Libre) o de Código abierto Programas que se pueden bajar desde Internet sin cargo.

FTP Protocolo de transferencia de Archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.

AEFCM Autoridad Educativa Federal en la Ciudad de México es un Órgano administrativo desconcentrado de la Secretaría de Educación Pública.

Firewall Es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial. Considerado también, como un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean, permite o deniega su paso. Para permitir o denegar una comunicación, el firewall examina el tipo de servicio al que corresponde, como pueden ser la Web, el correo o el IRC. Dependiendo del servicio, el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

Gusano Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.
Hardware Se refiere a las características técnicas y físicas de las computadoras.

Maltrato, descuido o negligencia Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la AEFCM.

Medios Magnéticos (medios de almacenamiento) Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CDs, Cintas, Cartuchos, DVDs, etc.).

Mecanismos de seguridad o de control Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. Que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Password Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6-10 caracteres alfanuméricos.

Periféricos Se entiende como periféricos los aparatos auxiliares que se conectan a la unidad central de una computadora tales como: CD Writer, Impresoras, Digitalizadores, entre otros.

Respaldo Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Software Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.

USB Siglas de "Universal Serial Bus", unidad de almacenamiento.

Usuario Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal, o dispositivo (hardware).

Virus Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones, por correo electrónico o al compartir archivos o diskettes de computadoras.

Vulnerabilidad Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencionado o accidental.

Rosario Sánchez Ramos
Directora General de Planeación, Programación y Evaluación Educativa

Jorge Antonio Sánchez Galván
Coordinador Sectorial del Centro de Desarrollo Informativo "Arturo Rosenblueth"

Eduardo Flores Mejía
Director de Infraestructura del Centro de Desarrollo Informativo "Arturo Rosenblueth"

DIRECTORIO

Luis Humberto Fernández Fuentes

Titular de La Autoridad Educativa Federal en la Ciudad de México

Rosario Sánchez Ramos

Directora General de Planeación, Programación y Evaluación Educativa

Jorge Antonio Sánchez Galván

Coordinador Sectorial del Centro de Desarrollo Informativo "Arturo Rosenblueth.

Eduardo Flores Mejía

Director de Infraestructura del Centro de Desarrollo Informativo "Arturo Rosenblueth.

AEF CIUDAD MÉXICO

AUTORIDAD EDUCATIVA FEDERAL EN LA CIUDAD DE MÉXICO