6. LECTURA Y APROBACIÓN DEL PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA ALCALDÍA DE COYOACÁN (ANEXO 2)

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA ALCALDÍA DE COYOACÁN

ALCALDÍA DE COYOACÁN

Nombre del Documento	Plan de Contingencia de Tecnologías de la Información y Comunicación.
Fecha de Elaboración	17 de Octubre de 2025
Vigencia	3 años

MTRO. SALVADOR FRAUSTO NAVARRO	C. Cesar A. Sánchez Espinosa	L.I. J. Francisco Dorantes Campos
Elaboró	**Revisó**	**Autorizó**

INTRODUCCIÓN

La creación e implementación de herramientas, sistemas, procesos y nuevas tecnologías que han transformado la vida diaria de la sociedad en general, han creado soluciones y nuevas necesidades, en un mundo cada vez más dependiente de la tecnología. Las organizaciones pueden enfrentar situaciones de emergencia o crisis que puedan afectar a la infraestructura tecnológica. En específico la Alcaldía de Coyoacán, su infraestructura tecnológica enfrenta riesgos, desde fallos técnicos, ocasionados por ataques cibernéticos, desastres naturales y errores humanos, estas amenazas que pueden afectar la continuidad operativa por lo que es imperativo contar con un Plan de Contingencia de Tecnologías de la Información y Comunicación.

Un Plan de Contingencia de Tecnologías de la Información y Comunicación es un conjunto de procedimientos y estrategias diseñadas para responder eficazmente ante situaciones de emergencia o crisis que a puedan afectar a la infraestructura tecnológica con la que cuenta la Alcaldía de Coyoacán. El plan de contingencia es herramienta esencial para mitigar estos riesgos y amenazas, asegurando que se pueda responder de manera efectiva a cualquier incidente que comprometa la infraestructura tecnológica.

El presente plan tiene como objetivo principal definir un conjunto de procedimientos y acciones a seguir para garantizar la continuidad de los servicios informáticos en caso de interrupciones inesperadas. Este plan describe las medidas preventivas, los procedimientos de respuesta ante incidentes y las estrategias de recuperación que permitirán a la organización minimizar el impacto de cualquier contingencia de Tecnologías de la Información y Comunicación y restaurar sus operaciones en el menor tiempo posible.

Este documento está dirigido a todos los usuarios de la infraestructura tecnológica de la Alcaldía de Coyoacán. La implementación exitosa de este plan requiere la colaboración de todos los usuarios, así como la actualización y revisión periódica para adaptarse a nuevas amenazas y cambios en la infraestructura tecnológica.

A través de este Plan de Contingencia de Tecnologías de la Información y Comunicación, se busca detectar los riesgos, evaluarlos, así como su impacto, estableciendo medidas para minimizar los daños, asegurando la continuidad de las operaciones, proteger sus tecnologías de la información y comunicación, asegurando la integridad y disponibilidad de la información.

OBJETIVO

Establecer un plan de contingencia de Tecnologías de la Información y Comunicación para la alcaldía de Coyoacán, minimizando los daños, asegurando la continuidad de las operaciones de la infraestructura tecnológica, la protección de la información, así como evaluar, analizar, prevenir los riesgos informáticos que puedan dar la suspensión completa o parcialmente de la prestación del servicio, todo esto en cumplimiento de las disposiciones legales aplicables a la Alcaldía de Coyoacán.

ALCANCE.

Este plan de contingencia es un análisis de posibles riesgos y amenazas a los cuales se encuentra sujeta la infraestructura de la alcaldía de Coyoacán, así como las acciones a seguir para reducir la probabilidad que ocurran o se ocasionen, como los procedimientos y estrategias para responder eficazmente ante estas situaciones, tomando en cuenta los recursos que conforman las Tecnologías de la Información y Comunicación de este órgano desconcentrado.

Las actividades consideradas en este documento son:

- Análisis de Riesgos
- Medidas Preventivas
- Previsión de Desastres Naturales
- Plan de Respaldo
- Plan de Recuperación

DEFINICIONES

Amenaza: Cualquier evento con probabilidad de ocurrencia, durante un período de tiempo específico y dentro de un área determinada, que pueda interferir con el funcionamiento de la infraestructura de Tecnologías de la Información y Comunicación, difusión de información no deseada u autorizada, fenómeno que puede potencialmente causar daños como fallas en el suministro eléctrico, virus, errores humanos, sabotaje informático, desastres naturales.

Ataque: Acción o evento que interfiera con la continuidad del funcionamiento adecuado de la infraestructura de Tecnologías de la Información y Comunicación, puede ser también una intromisión remota no autorizada para obtener información contenida dentro de esta infraestructura.

Base de datos: Conjunto de datos organizados entre los cuales existe una correlación y que además están almacenados con criterios, archivos interrelacionados manejados y creados en un sistema de administración

Contingencia: Evento o suceso que ocurre de forma natural o por la sociedad, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

Datos de información: Conjunto de datos que se resguardan en los servidores de archivos y que por seguridad y confidencialidad no pueden ser modificados, ni eliminados.

Documentación: Comprende todos aquellos oficios, registros y documentos que avalan los procedimientos de acciones tendientes a mejorar la operación de Tecnologías de la Información y Comunicación, solicitudes de servicio y equipamiento realizados por usuarios, licenciamiento en papel del software que avalan la propiedad de la Alcaldía, así como Anexos, Justificaciones y Dictámenes Técnicos emitidos por la Comisión de Gobierno Electrónico - CGE-.

Equipo de telecomunicaciones: Son los equipos que permiten la interconectividad de todo el edificio central, así como de los, y la correcta distribución de servicios de datos, voz e Internet (en algunos casos son equipos proporcionados por el proveedor del servicio).

Gravedad: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

Hardware: Medios físicos que se ocupan para el desarrollo de las actividades propias del área, como son Servidores de datos, portal WEB y de Correo, Ruteadores, Switch's y equipos de telecomunicación.

Incidente: Es la ocurrencia de uno o varios eventos que atentan contra la confiabilidad, la integridad y la disponibilidad de la información y que violan las medidas de seguridad de la infraestructura de Tecnologías de la Información y Comunicación, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

Riesgo: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

Seguridad de la Información: La seguridad de la información se comprende a través de la disponibilidad, integridad y confidencialidad en cual consiste en medidas y procedimientos encaminados al cumplimento en los objetivos que se describen.

Suministro de energía eléctrica: Contiene todas las Unidades de Respaldo de Energía (UPS), así como los no-break que se encuentran en el MDF e IDF's, para garantizar el suministro de energía eléctrica de los servidores, switch's y ruteadores.

a) ANÁLISIS DE RIESGOS

Para el análisis de riesgos debemos identificar, evaluar e implementar acciones sobre amenazas que pueden interrumpir la operación de la infraestructura de Tecnologías de la Información y Comunicación de la Alcaldía de Coyoacán en cualquiera de los sitios que integran la misma, como son los siguientes:

a) Imposibilidad de acceso físico a los recursos informáticos debido a problemas en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese, por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
c) Divulgación de información a instancias no autorizadas, fuera de la Alcaldía que afecten su patrimonio estratégico e institucional, ya sea mediante Robo o Ingeniería Social.
d) Identificar el tipo de amenazas como las siguientes que son enunciativas mas no limitativas:

Identificación de Amenazas		
No.	**Amenaza**	**Tipo**
01	Terremoto/ sismo.	Siniestros Naturales
02	Inundación en el Centro de Datos y Comunicación (Edificio Centralizado).	
03	Incendio.	
04	Falla en telecomunicaciones.	Tecnológico
05	Delito informático.	
06	Falla de hardware y software.	
07	Falla de suministro eléctrico.	Físico y Ambiental
08	Mal uso de los bienes informáticos.	Humano
09	Pandemia y/o Epidemia.	A la Salud

b) PRIORIDADES.

La estimación y valoración de los daños o amenazas en los bienes y su impacto, fija la prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios que se pierden en el acontecimiento. Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de contingencia.

c) ELEMENTOS, SITUACIONES O CONDICIONES QUE CAUSEN LOS DAÑOS.

Los elementos, situaciones o condiciones que ocasionen posibles daños, que pueden causar el mal funcionamiento de la red de datos de la Alcaldía de Coyoacán en cualquiera de los sitios que integran la misma, pueden ser acciones de forma directa o indirecta como lo son las siguientes:

Acciones Directas

- Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).
- Ruptura de las claves de acceso a los sistemas computacionales.
- Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).
- Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.
- Robo de equipo de información.
- Virus informáticos.

Acciones Indirectas

- Fallas de la planta de luz.
- Fallas de los equipos de acondicionamiento atmosféricos necesarios para una adecuada operación de los equipos computacionales más sensibles.
- Por fallas de la comunicación (proveedor externo).
- Por fallas en el tendido físico de la red local.
- Fallas en las telecomunicaciones con instalaciones externas.
- Por fallas de Central Telefónica.
- Cuestiones naturales (Movimientos telúricos, Inundaciones, incendios, cortocircuitos, etc.).

d) MEDIDAS PREVENTIVAS

Realizar un levantamiento de los bienes informáticos

Realizar un Inventario del equipo de cómputo y comunicación, así como del software a fin de establecer puntualmente qué se tiene que resguardar. Adicional conocer y establecer los servicios de cómputo, telecomunicaciones, Internet. etc., indispensables para que los usuarios puedan llevar a cabo sus actividades esenciales.

Identificar las amenazas posibles

Para prevenir y aminorar las posibles consecuencias por fallas, daños o amenazas en los bienes informáticos de la Alcaldía de Coyoacán, con el fin de agilizar la reapertura del servicio y garantizar la operación de los mismos, se debe identificar el tipo de amenaza considerando lo siguiente:

Tipo de daño	Tipo de amenaza	Descripción	Prevención
Alta	Incendio por causas externas	Se percibe la destrucción de equipos y archivos.	Contar en el inmueble con extintores, aspersores, detectores de humo, asimismo, tener copias de respaldo.
	Terremoto, Sismo o Inundaciones	Se percibe la destrucción de equipos y archivos.	Contar con copias sea por medios de respaldo como la nube, USB o discos duros.
Media	Fallas en el Hardware	Se percibe la perdida de archivos debido por sobrecalentamiento, plagas, golpes de impacto o caída.	Estar atento al mantenimiento, equipos de respaldo, garantías y copias de respaldo.
	Fallas en el Software	Se percibe daños a equipos y archivos por virus, errores en el sistema, fallos al sistema de archivos.	Realizar actualizaciones del sistema operativo, Antivirus actualizados, copias de respaldo.

Tipo de daño	Tipo de amenaza	Descripción	Prevención
Media	Vandalismo	Daños a equipo informático	Seguro contra todo riesgo, copias de respaldo.
Alta	Robo de información	Afectación a la integridad de los datos sin la debida autorización o acceso permitido.	Estar alerta y ratificar el cambio de claves de acceso mínimo cada seis meses, así como la protección de las copias de respaldo.
Alta	Pandemia	Afectaciones a la salud del personal el cual produce afectación interrupción al servicio público.	Implementar protocolos de salud y seguridad asimismo puede requerir recursos adicionales y de reorganización del espacio de trabajo.
Baja	Incidente o Uso inapropiado de los bienes informáticos	Afectación por la navegación a sitios web no relacionados con el trabajo durante el horario laboral.	Tener en constante capacitación al usuario, así como actuar con forme políticas de seguridad y contar copias de respaldo.
Media	Falla por suministro eléctrico	Falla en la planta de energía eléctrica o bien de un equipo generador de respaldo o no-break.	Realizar evaluaciones de riesgo para la identificación de vulnerabilidades en el suministro eléctrico y desarrollar estrategias de mitigación.

e) PLAN DE RESPALDO

Todos los servidores son considerados críticos, ya que de su óptimo funcionamiento depende la estabilidad de los servicios e información que emana para el desarrollo de las actividades propias de la Alcaldía de Coyoacán, los más importantes son:

a) Servidor Proxy (Filtro que proporciona el servicio de Internet en el Edificio Central.
b) Servidor Firewall (Filtro que proporciona el servicio de Internet en el Edificio de Datos de la Alcaldía de Coyoacán Servidores de Página WEB y Correo.

c) Servidores de Aplicaciones Administrativas (Control de Gestión, Control de Personal, Órdenes de Servicio).

f) PLAN DE RECUPERACIÓN

Se atenderá adecuadamente, pronta atención y recuperación a las fallas, daños o amenazas de los bienes informáticos de la Alcaldía de Coyoacán, con la finalidad de proporcionar soluciones que garanticen la operación de los mismos.

Los objetivos del plan de Recuperación son:

1. Apego a las políticas y procedimientos existentes para llevar a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento.

2. Lograr la reactivación dentro de las 12 horas de producida una contingencia mayor, de todo el sistema de procesamiento, servicios y sus funciones asociadas, a un nivel básico de operación.

3. Permanente mantenimiento y supervisión de los sistemas, aplicaciones y equipos relevantes para la operación correcta de los servicios.

4. La correcta aplicación de las acciones a realizar para garantizar una rápida y oportuna respuesta frente a una contingencia.

Alcance del Plan de Recuperación

Restablecer en el menor tiempo posible el nivel de operación de la infraestructura de Tecnologías de la Información y Comunicación, basándose en los planes de emergencia y de respaldo a los niveles del nodo central (Edificio Central) y de los demás sitios (Edificios de la Alcaldía de Coyoacán).

La responsabilidad sobre el Plan de Recuperación es de la Dirección de Gobierno Digital, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

Activación del plan.

La Dirección de Gobierno Digital implementará el Plan de Contingencia de Tecnologías de la Información y Comunicación, podrá indicar un lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en la magnitud y las afectaciones resultantes de la misma.

Duración estimada

De acuerdo al tipo de fallas se determinará la duración de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado a un lugar alternativo.

Existen diferentes tipos de contingencia de acuerdo al daño sufrido:

1. Baja. Tiene repercusiones sólo en la operación diaria.
2. Media. Causa daños a las instalaciones, pero pueden retomar las operaciones.
3. Alta. Incluye ambas, afecta la operación e instalaciones y no pueden ser recuperables en corto tiempo.

g) CONSIDERACIONES ADICIONALES

- El Plan de contingencia de Tecnologías de la Información y Comunicación se revisará ante el comité de Tecnologías de la Información y Comunicación cada tres años o cuando las condiciones así lo requieran.

- Frente a la contingencia, se notificará a la Jefatura de la Alcaldía de Coyoacán y a su vez a la Subdirección de Tecnologías de la Información y Comunicación ya que será la que deberá evaluar en el sitio, la magnitud de la misma, estimando el tiempo de paro de operaciones, mientras se lleva a cabo las acciones de recuperación.

- La Dirección de Gobierno Digital determinará el lugar donde se instalará el sistema alternativo (red y servidor alterno), pudiendo ser en las mismas instalaciones del desastre, si las condiciones lo permiten, o en instalaciones externas que cuenten con los requerimientos necesarios para implementar el Plan de Contingencia de Tecnologías de la Información y Comunicación y restaurar la conectividad.

- Se tomará nota de las condiciones de la nueva plataforma operativa (sus capacidades y limitaciones, tanto en funcionalidad como en velocidad), e informará a los usuarios para operar de acuerdo a estas restricciones, durante el tiempo que se vuelve a reestablecer el nivel de operaciones normales.

- La Dirección de Gobierno Digital, asignará personal necesario, para las tareas de recuperación e informará el estatus de avance en cada proceso del plan, a la Jefatura de la Alcaldía de Coyoacán.

h) GUIA DE ACCIONES.

Tipo de daño	Tipo de amenaza	Prevención
Baja	Incendio: destrucción de equipos y archivos.	Extintores, aspersores automáticos, detectores de humo, pólizas de seguros.
Alta	El robo común: pérdida de equipos y archivos.	Copias de respaldo (BackUp), Seguros sobre robos de equipos y contra todo riesgo, alarmas.
Media	Vandalismo: daño a los equipos y archivos	Seguro contra todo riesgo, copias de respaldo
Media	Fallas en los equipos: daño a los archivos.	Mantenimiento, equipos de respaldo, garantía y copias de respaldo.
Media	Equivocaciones: daño a los archivos.	Capacitación, copias de respaldo, políticas de seguridad.
Alta	Acción de Virus: daño a los equipos y archivos	Actualizaciones del sistema operativo, Antivirus actualizados, copias de respaldo
Baja	Terremotos: destrucción de equipo y archivos	Seguro contra todo riesgo, copias de respaldo.
Alta	Accesos no autorizados: filtrado no autorizado de datos	Cambio de claves de acceso mínimo cada seis meses. Política de seguridad para acceso a personal competente.
Media	Robo de datos: difusión de datos sin el debido permiso o	Cambio de claves de acceso mínimo cada seis meses, custodia de

	acceso permitido.	las copias de respaldo.
Baja	Fraude: modificación y/o desvío de la información y fondos de la institución.	Sistemas de información seguros con dos usuarios para autorizar transacciones, procedimiento de control.

No.	Acción
1	Copias de seguridad de la información y documentos residentes en los discos duros.
2	Copias de seguridad de los sistemas de información y Bases de Datos
3	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de una computadora o servidor en caso de falla o virus.
4	Mantenimientos, revisiones preventivas y correctivas de equipos de cómputo y comunicación, extintores, alarmas y sistemas contra incendio, para mantenerlos en óptimas condiciones.
5	Actualizar las claves o contraseña de acceso a las aplicaciones y bases de datos.
6	Mantener actualizados los sistemas operativos, antivirus y aplicaciones
7	Mantener como respaldo un inventario adicional con equipos de cómputo, repuestos, consumibles, para su reemplazo.

I) ACCIONES ANTE EMERGENCIAS.

a) EMERGENCIA FÍSICA EN SERVIDOR

1. Error Físico de Disco de un Servidor.

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

a. Ubicar el disco crítico.
b. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
c. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
d. Bajar el sistema y apagar el equipo.

e. Retirar el disco dañado y reponerlo con otro del mismo tipo, formatearlo y darle partición.
f. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
g. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
h. Habilitar las entradas al sistema para los usuarios.

2. Error de Memoria RAM

En este caso se dan los siguientes síntomas:

i. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
j. Ante procesos mayores se congela el proceso.
k. Arroja errores con mapas de direcciones hexadecimales.
l. El servidor deberá contar con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.
m. Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.
n. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias dañadas.
- Retirar las memorias dañadas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Probar los sistemas que están en red en diferentes estaciones.
- Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

3. Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

o. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
p. El servidor debe estar apagado, dando un correcto apagado del sistema.
q. Ubicar la posición de la tarjeta controladora.
r. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
s. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
t. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
u. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

4. Caso de Incendio Total

La mejor manera de **prevenir** un incendio es no provocarlo. Observe las prohibiciones de no fumar y las normas de prevención institucional.

En presencia del fuego tenga en cuenta que:

- Puede tratar de apagar un fuego en una oficina siempre que tenga detrás una puerta que le permita salida.
- Si el fuego prende en sus ropas, no corra, tírese al suelo y ruede. Si el hecho ocurre a otra persona cúbrala con alguna prenda o con una toalla humedecida, si se encuentra próximo a un aseo. No se quite la ropa si tiene quemaduras.
- En presencia de aparatos eléctricos, no eche agua al fuego. Tampoco debe hacerlo ante líquidos inflamables (alcohol, aceite, gasolina, etc).
- Si hay mucho humo póngase un pañuelo en la boca y nariz, a ser posible mojado, y salga agachado o gateando. Respire profundamente para evitar desvanecimientos.
- Al salir de la dependencia, procure cerrar las ventanas y las puertas, pues las corrientes avivan el fuego.

- Si se encuentra aislado y no puede ponerse a salvo, diríjase a la habitación más alejada del fuego (pero no a un nivel superior a menos que esté seguro de que los equipos de rescate se encuentran muy cerca y provistos de escaleras largas u otro equipo.
- Si se ve obligado a huir a través de las llamas para ponerse a salvo, no se entretenga en recoger nada, cúbrase (incluyendo la cabeza) con una manta, una toalla, una cortina o un abrigo mojados si es posible, luego aguante la respiración y corra.
- Si tiene que desalojar el edificio siga las normas de "Evacuación".

5. Caso de Inundación

v. Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.
w. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
x. Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.
y. Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.
z. Proveer cubiertas protectoras para cuando el equipo esté apagado.

6. Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

aa. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.
bb. Las tareas de supervisión y vigilancia de funcionamiento de los servidores tras el incidente y/o falla eléctrica, están a cargo por personal designado por el titular del Área de Tecnologías de la Información y Comunicación de la Secretaría de Salud.

7. Generalidades con respecto a la seguridad ante emergencia

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos.

cc. Ante todo, se debe conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, se debe tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

dd. Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

b) EMERGENCIAS DE DATOS (CASO)

1. Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

a. Contar con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación.
b. El antivirus muestra el nombre del archivo infectado y quién lo usó.
c. Si los archivos de sistema han sido afectados por el virus, estos archivos serán reemplazados del disco original de instalación o del backup.
d. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras:

Se revisará las computadoras y laptops con antivirus preferentemente portable.

De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

a. Utilizar un antivirus (preferentemente portable en usb o cd) igual o mayor en versión al instalado en la computadora infectada. Reiniciar la computadora con dicho dispositivo portable.
b. Retirar el dispositivo portable con el que arrancó la computadora e insertar el antivirus portable, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, se borrará el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del escaneado. Finalizado el escaneado, reconstruir el Master Boot del disco duro.

c. En cualquier caso de que se realice el escaneo de equipos de cómputo y/o laptops por fallas o daños causados por virus, se debe realizar un respaldo de archivos y documentos, esto en la medida de lo posible y si así lo permite el equipo de cómputo.

c) RESPECTO A LA ADMINISTRACIÓN DE LOS BACKUPS

a. Se administrará bajo la lógica de un almacén, esto implica ingreso y salida de medios magnéticos (USB, discos removibles, CD's, etc.) obviamente teniendo más cuidado con las salidas y cuidando que el grado de temperatura y humedad sean los adecuados.
b. Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.
c. El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

d) RESPECTO A LA ADMINISTRACIÓN DE IMPRESORAS

a. Todo listado que especialmente contenga información confidencial, debe ser destruido.
b. Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
c. Establecer controles respecto a los procesos remotos de impresión.

e) PARA EL MANTENIMIENTO DE LOS DISCOS DUROS

a. Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
b. El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.
c. Evitar que la computadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.
d. No mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.
e. para mantener la velocidad en el equipo, se debe realizar una vez al mes el proceso de desfragmentación para conservar en óptimo estado la respuesta del equipo; Windows incluye un Desfragmentador de disco fácilmente
f. Localizable en el menú Inicio/Todos los programas/Accesorios/Herramientas del Sistema/Desfragmentador de disco.
g. Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un equipo de cómputo.

f) RESPECTO A LOS MONITORES

a. Usar medidas contra la refección para reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día.
b. Sentarse por lo menos a 60 cm. de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.
c. También manténgase por lo menos a 1 m. o 1.20 m. del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.
d. Finalmente apague su monitor cuando no lo esté usando

g) PARA EL CUIDADO DEL EQUIPO DE CÓMPUTO

a. Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función. Para eliminar el polvo del teclado, lo más conveniente es voltearlo y soplar el aire comprimido para que éste salga completamente. Se debe evitar en lo posible quitar las tapas de las teclas de la PC para lavarlas, ya que su reposición puede generar fallas mecánicas.
b. Mouse. El mouse percibe los movimientos a través de una esfera de caucho, la cual mueve dos rodillos; por lo general, en éstos se acumula suciedad con el uso, impidiendo el correcto funcionamiento, para limpiarlos se debe quitar con cuidado la tapa para liberar la esfera y usar un hisopo para limpiar los rodillos. Antes de realizar cualquier movimiento, se sugiere observar cómo están colocados, por si ocurre algún accidente, no haya ningún problema para colocarlos nuevamente. Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste. Para el caso de Mouse de led alejarlo de zonas con polvo y se recomienda el uso de mouse pad.
c. CD-ROM. Antes de usar cualquiera de estos componentes, se debe verificar que el CD-ROM/DVD o CDRW del equipo se encuentren limpios, de igual forma, cada CD o DVD que se utilicen deben encontrarse libres de polvo y partículas para forzar menos al láser y prolongar su duración.
d. Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.
e. Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones y cuidar el cambio de cartuchos de tinta/ tóner.
f. En caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado. Papelera de reciclaje. Windows reserva un 10 por ciento de la capacidad del disco duro para mantener algo de la información que ya se haya eliminado, con la finalidad de que en cualquier momento se pueda recuperar. No obstante, la papelera de reciclaje, ubicada en el Escritorio de la computadora, debe limpiarse con regularidad para no llenarse de basura que le estará quitando espacio en disco duro.
g. Se debe seleccionar el ícono y hacer clic derecho, posteriormente elegir la opción Explorar, podrá ver todos los archivos ubicados en su papelera y eliminar aquéllos que no necesite o, en su caso, vaciar la papelera de reciclaje.

h. Término de sesión o apagado. En muchas ocasiones, por la prisa o mal uso de la computadora, no se cierran las aplicaciones correctamente o bien, no se apaga la computadora de forma adecuada, esto provoca pérdida de información y daña el sistema operativo.

h) MANTENER LA S ÁREAS OPERATIVAS LIMPIAS Y PULCRAS

a. Para proteger a nuestras computadoras del polvo, resulta muy conveniente adquirir algunas fundas para los CPU, monitor, teclado, escáner, y/o cualquier otro equipo de cómputo para evitar que entre el polvo a los componentes más sensibles y cause daño; no se debe olvidar que la limpieza es necesaria, para ello se pueden emplear aire comprimido, espumas y una pequeña franela (Soporte técnico).

i) REPORTE DE PROBLEMA Y SOLICITUD DE MEJORA

a. Los funcionarios y/o personal de la institución pueden solicitar la solución de un problema presentado o realizar una solicitud de mejora del sistema o percance presentado, comunicándolo al Área de Tecnologías de la Información y Comunicación quienes son los encargados de gestionar cualquier solicitud por parte de los usuarios finales, presentando una solución de acuerdo con el nivel de importancia, los niveles de servicio y tipo de problema presentado.

PRESIDENTE

Lic. Jonathan Evani Flores Simbrón
Director General de Planeación del Desarrollo, Gobierno Abierto y Ordenamiento Territorial

SECRETARÍA TÉCNICA

L.I. Juan Francisco Dorantes Campos
Director de Gobierno Digital

VOCAL

Lic. Roberto Sánchez Lazo Pérez
Director General Jurídico y de Gobierno

SUPLENTE

C. Saúl Rodríguez Cabello
Subdirector de Control y Seguimiento de Jurídico y Gobierno

VOCAL

Arq. Martha Amalia Elguea Viniegra
Directora General de Obras Públicas y Desarrollo Urbano

SUPLENTE

P.T. Marla Isel González Morales
Subdirectora de Control y Seguimiento de Obras Públicas y Desarrollo Urbano

VOCAL	SUPLENTE
C. Juan Manuel Cortes Rico Director General de Servicios Urbanos	Lic. Ameiatzin Quetzalli Guerrero Maldonado Subdirectora de Control y Seguimiento de Servicios Urbanos
VOCAL	**SUPLENTE**
MD. Fernando Daniel Cravioto Padilla Director General de Desarrollo Social y Fomento Económico	Lic. Vanessa Jocelyn Uribe Mejía Directora de Desarrollo Humano
VOCAL	**SUPLENTE**
Mtra. Aurora Monserrat Cruz Ramírez Directora General de Seguridad Ciudadana	Mtra. Verónica del Valle Ramos Subdirectora Control y Seguimiento de Seguridad Ciudadana

VOCAL	SUPLENTE
Lic. Iliana Beatriz Pardo Hernández **Directora General de Participación Ciudadana**	**Lic. Margarita Belén Olivas García** **Subdirectora de Control y Seguimiento de Participación Ciudadana**
VOCAL	**SUPLENTE**
Mtra. Hilda Trujillo Soto **Directora General de Cultura**	**Lic. Rodrigo Antonio Pineda Arenas** **Jefa de Unidad Departamental de Fomento de Casas de Cultura**
VOCAL	**SUPLENTE**
Mtra. Desirée Guadalupe Navarro López **Directora General de Derechos Humanos y Grupos Prioritarios**	**C.P. Lorena Cobos Cruz** **Subdirectora de Control y Seguimiento de Derechos Humanos y Grupos Prioritarios**

VOCAL	SUPLENTE
Mtra. Maricarmen Hernández Gutiérrez **Directora General de Administración y Finanzas**	
INVITADO/A/S PERMANENTE/S	**INVITADO/A/S PERMANENTE/S**
C. César Ariel Sánchez Espinosa **Subdirector de Tecnologías de la Información y Comunicación**	**Mtro. Salvador Frausto Navarro** **Subdirector de Innovación Tecnológica**
INVITADO/A/S PERMANENTE/S	**INVITADO/A/S PERMANENTE/S**
C. Luis Felipe Mendiola González **Jefe de Unidad Departamental de Apoyo y Soporte Técnico**	**C. Humberto Villegas Galván** **Jefe de Unidad Departamental de Sistemas Informáticos**

INVITADOS/AS

Lic. Jazmín Dolores Muñoz García
Titular del Órgano Interno de Control en la Alcaldía Coyoacán

INVITADOS/AS

Lic. Kareen Maqueda Vera
Jefa de Unidad Departamental de Mecanismos Anticorrupción

INVITADOS/AS

Mtro. Federico Manzo Sarquis
Coordinador de la Unidad de Transparencia