PLAN DE CONTINGENCIA INFORMÁTICA

ALCALDÍA COYOACÁN

SUBDIRECCIÓN DE INFORMÁTICA

Nombre del documento	Plan de Contingencia Informática
Fecha de elaboración	Septiembre 2022
Vigencia	2 años

María Magdalena Sánchez López	Isaac Huerta Castillo	José Alberto Juarez Ríos	Sergio Javier Riveroll Arellano
Elaboró	Revisó	Revisó	Autorizó

La seguridad informática son las medidas y procedimientos encaminados al cumplimiento de tres objetivos:

1. La continuidad del trabajo. Mantener funcionando el sistema en todo momento estableciendo mecanismos que permitan un ritmo de trabajo aceptable en tanto se soluciona el problema.

2. Integridad de la información. Que el usuario tenga oportunamente la información para el desarrollo de sus actividades.

3. Confidencialidad de los datos. Cada usuario tendrá acceso exclusivamente a la información que le corresponde y compete.

Este Plan de Contingencia Informática se elaboró considerando evaluar las situaciones de riesgo y definir las tareas orientadas a reducir dichos riesgos a la infraestructura informática y los procedimientos relevantes de la plataforma tecnológica que se utilizan en la Alcaldía de Coyoacán.

Se debe entender como infraestructura informática al hardware, software y elementos complementarios que soportan la información para la función de la Red de Datos de la Alcaldía de Coyoacán. También se relacionan los procedimientos relevantes a la infraestructura informática, todas aquellas tareas que su personal realiza frecuentemente cuando interactúa con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

1. Planificación de Contingencia

La seguridad de datos consiste en un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. La seguridad es un elemento básico para garantizar la conservación de la información y bienes informáticos, así como entregar el mejor servicio a los usuarios, considerando a la información como uno de los activos más importantes de la Alcaldía de Coyoacán: lo cual hace que la protección de esta sea el fundamento más importante de este Plan de Contingencia.

En este documento se resalta la necesidad de contar con estrategias que permitan realizar: análisis de riesgos, de prevención, de emergencia, de respaldo y recuperación de datos.

d) 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.

e) Documentación

Comprende todos aquellos oficios, registros y documentos que avalan los procedimientos de acciones tendientes a mejorar la operación informática, 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 –.

f) 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.

g) Equipo de telecomunicaciones

Se refiere a 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).

2.2. Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos 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 fuera de la Alcaldía que afecten su patrimonio estratégico e institucional, ya sea mediante Robo o Ingeniería Social.

MEDIA ALTA	Daño en software de arranque o programas de servidores de archivos	Acción Media
MEDIA ALTA	Falla en el suministro de energía eléctrica, atribuible a causas externas a las instalaciones de la Alcaldía de Coyoacán. (Se soportará con el equipo de respaldo, hasta un máximo de 2 horas)	Acción Media (1 a 3 horas) depende del proveedor externo
MEDIA	Falla en la integridad de los datos que se ocupan para realizar reportes o informes de los servidores.	Acción Media (3 a 4 horas)

2.4. Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operacion normal de la red de datos de la Alcaldía en cualquiera de los sitios que integran la misma, pueden ser los siguientes:

Acciones Directas

1) Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).

2) Ruptura de las claves de acceso a los sistemas computacionales.

3) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).

4) Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

5) Robo de equipo de información.
6) Virus informáticos

Fallas de Hardware

a) Falla en el Servidor de Aplicaciones y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.

b) Falla en el hardware de Red:

- Falla en los Switches.
- Falla en el cableado de la Red.

e) Falla en el Router.

d) Falla en el FireWall (Edificio)

e) Falla en el Proxy (Centro de Datos)

f) Falla en el conmutador (Proveedor externo)

2.5. Expectativa Semestral de Daños

Se realizarán evaluaciones semestrales, considerando las pérdidas de información y fallas atendidas, a efecto de tomar las medidas precautorias necesarias para que el tiempo de recuperación y puesta en marcha, sea menor o igual al necesario para la reposición del equipamiento que lo requiere o lo soporta.

Medidas Preventivas

3.1 Realizar un levantamiento de los bienes informáticos

1. 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.

3.2 Identificar las amenazas posibles

2. Identificar los tipos se siniestros a los cuales esta propenso cada uno de los procesos críticos, como falla eléctrica, incendio, terremoto.

Seguridad Física del Personal

Se tomaron medidas a fin de que el personal comparta sus conocimientos entre sí, en lo referente a la utilización del software y elementos de soporte relevantes. Estas acciones permiten mejorar los niveles de seguridad, favoreciendo los reemplazos en caso de contingencia, emergencias o períodos de ausencia ya sea por vacaciones o enfermedades.

Seguridad de la Información

La información y programas de los Sistemas de Información que se encuentran en los Servidores o en otras estaciones de trabajo críticas, están protegidas mediante claves de acceso y a su vez un plan de respaldo adecuado.

Asimismo, y a fin de garantizar la calidad y el acceso a la información, habrá que tomar medidas sobre la destrucción de archivos, su modificación y/o divulgación. En este caso es conveniente que los usuarios sean conocedores de los procedimientos para evitar los problemas derivados de los riegos anteriores.

5. Plan de Respaldo

El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Todos los nuevos diseños de Sistemas, Proyectos o ambientes, tendrán sus propios Planes de Respaldo.

Respaldo de datos Vitales

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)

Activación del Plan

Decisión

Queda a juicio de la Subdirección de Informática determinar la activación del Plan de Contingencia, e indicar el 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. Para este caso se deben considerar las prioridades anteriormente citadas.

Existen diferentes tipos de contingencia de acuerdo al daño sufrido:

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

Responsabilidades

- Orden de Ejecución del Plan: Subdirección de Informática
- Supervisión General de Plan: Subdirección de Informática
- Supervisión del Plan de Recuperación: Supervisor de la red y plataforma informática.
- Abastecimiento (HW, SW): Personal de la JUD de Redes y Desarrollo de Sistemas.
- Tareas de Recuperación: Personal de tareas afines.

Personal Clave

Es el responsable de la aplicación de los procedimientos que describa el Plan de Contingencia para cada una de las diferentes circunstancias o contingencias previstas

Aplicación del Plan

Se aplicará el Plan de Contingencia Informática siempre que se prevea una pérdida de servicio por un periodo mayor de 48 horas, en los casos que no sea un periodo de evaluaciones, inscripciones, etc.; y un período mayor a 24 horas durante los periodos de actividades ordinarias, tomando en consideración también el sitio donde se origine la contingencia.

Consideraciones Adicionales

1. El Plan de Contingencia Informática deberá ser revisado una vez al año.

Frente a la contingencia, se notificará a la Jefatura de la Alcaldía de Coyoacán y a su vez la Subdirección de Informática evaluará en sitio la magnitud de la misma, estimando el tiempo de paro de operaciones mientras se lleva a cabo las acciones de recuperación.

Si el tiempo estimado es mayor a 48 horas de interrupción de operaciones en cualquier día salvo durante el periodo de actividades establecidas en calendario escolar, en cuyo caso el tiempo estimado no será mayor a 24 horas, entonces convocará al personal asignado para ejecutar la recuperación, compuesto por:

* Supervisión General de Plan: Subdirección de Informática
* Supervisión del Plan de Recuperación: Supervisor de la red y plataforma informática.
* Abastecimiento (HW, SW): Personal de la JUD de Apoyo y Soporte Técnico.
* Tareas de Recuperación: Personal de tareas afines.

En reunión extraordinaria se 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 Informática y restaurar la conectividad.