



PLAN DE CONTINGENCIA TECNOLÓGICA DEL INSTITUTO MUNICIPAL DE LAS MUJERES DE LEÓN, GUANAJUATO

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

Objetivo

Este documento establece un Plan de Contingencia Informático para el Instituto Municipal de las Mujeres de León, Guanajuato. Su propósito es definir un proceso de recuperación ante posibles contingencias que afecten los equipos de cómputo, asegurando la rápida y efectiva restauración de los servicios con el menor impacto posible.

Alcance

El presente Plan de Contingencia Tecnológica tiene como objetivo prevenir y gestionar emergencias que puedan afectar los equipos de cómputo, la red y los sistemas de información del Instituto Municipal de las Mujeres de León, Guanajuato, tanto por causas internas como externas. Este plan se desarrolla a partir de un análisis de riesgos.

Glosario

Contingencia: Posibilidad de que algo suceda o no.

Equipo de cómputo: Dispositivo electrónico diseñado para procesar datos y realizar tareas específicas mediante la ejecución de programas.

Energía (Uninterruptible Power Supply): Sistema de Alimentación Ininterrumpida, (UPS) dispositivo que proporciona energía eléctrica de respaldo a equipos electrónicos en caso de un corte de luz o una falla en el suministro eléctrico.

Red: Conjunto de dispositivos (como computadoras, servidores, impresoras, etc.) interconectados entre sí, que pueden comunicarse y compartir recursos entre ellos. Estos dispositivos intercambian datos y recursos a través de medios físicos o inalámbricos, utilizando protocolos de comunicación.

Sistema de información: Conjunto organizado de componentes que trabajan juntos para recopilar, procesar, almacenar y distribuir información.

Sistema No-Break: Sistema de alimentación ininterrumpida.

SITE: Se les llama así también a los centros de datos que son el espacio físico en el que se almacena y administra los equipos informáticos necesarios para la operación de los sistemas de información del Instituto Municipal de las Mujeres de León, Guanajuato.

Atención ante contingencias tecnológicas

En caso de presentarse una contingencia relacionada con los servicios de tecnologías de la información, se evaluará la situación para determinar la mejor forma de atención, considerando las siguientes alternativas:

- ✚ Asistencia telefónica.
- ✚ Soporte remoto mediante herramientas de control remoto autorizadas.
- ✚ Asistencia presencial, especialmente en casos de fallas de red o situaciones que lo ameriten.

Procedimiento:

1. Atención telefónica a los usuarios (registro de la solicitud).
2. Validación del tipo de falla o incidente reportado.
3. Resolución del problema mediante el medio más adecuado.
4. Confirmación con el usuario sobre la solución del incidente.
5. Cierre del caso.

Resguardo de información sensible

La información generada y almacenada en los equipos de cómputo es responsabilidad de cada persona funcionaria pública. No obstante, la Unidad de Tecnologías de la Información brinda apoyo para el respaldo de información sensible, con el objetivo de prevenir pérdidas ante contingencias.

Procedimiento:

1. Cada persona funcionaria pública es responsable del resguardo de su información laboral.

2. Se ofrecerá respaldo de información en el servidor ubicado en el SITE del Instituto previa solicitud por correo a: ti.immuleon@gmail.com
3. La periodicidad de los respaldos será semanal.
4. En caso de pérdida de datos por contingencia, se restaurará la copia de seguridad más reciente disponible anterior al evento.

Suministro de energía eléctrica y sistemas de respaldo

Ante una interrupción en el suministro eléctrico, se cuenta con sistemas de respaldo que permiten continuar con las funciones esenciales por un tiempo limitado.

Procedimiento:

1. Identificación del fallo en el suministro eléctrico (por parte de Comisión Federal de Electricidad).
2. Activación automática del sistema No-Break en los equipos que cuentan con él.
3. Los No-Break en los equipos de las personas funcionarias públicas tienen una autonomía de entre 10 y 25 minutos, dependiendo del modelo y carga.
4. Si el corte de energía persiste y los sistemas de respaldo se agotan, se procede al apagado seguro de los equipos para evitar pérdida de información o daños.
5. Una vez restablecido el suministro eléctrico, se reinician los equipos y se reanudan las operaciones normales.