SISTEMA DE CONTROL INTERNO
JUÁREZ, HIDALGO

PLAN DE RECUPERACIÓN DE DESASTRES Y DE CONTINUIDAD DE LA OPERACIÓN PARA LOS SISTEMAS INFORMÁTICOS DE JUÁREZ HIDALGO

Elaboró	Autorizó
_____	_____
C. A. Julio Gustavo Aguilar García Contralor Municipal	C. Noé Zapata Sánchez Presidente Municipal Constitucional

Plan de Recuperación de Desastres y de Continuidad de la Operación para los Sistemas Informáticos del Municipio de Juárez Hidalgo, Hidalgo.

Introducción.

Un plan de recuperación de desastres y de continuidad de la operación, también conocido como plan de contingencia informático, es una metodología para la gestión de un buen manejo y administración de las Tecnologías de la Información y las Comunicaciones, para tener un pleno dominio del soporte y el desempeño de la infraestructura informática del municipio de Juárez Hidalgo.

Este plan debe tener las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las actividades del municipio. El plan se diseña para que en el caso de un siniestro se active de inmediato, permitiendo dar continuidad a las actividades y servicios de la institución.

Nuestro plan, deberá ser aplicado en primera instancia por el área de Informática, dado que en ésta área se encuentran los servidores de información, así como por cada usuario que a su vez tiene asignado un equipo de cómputo, propiedad del Municipio.

Para la elaboración de este plan, se deben considerar los siguientes puntos:

- Análisis y valoración de riesgo.

Se identifican las preocupaciones y prioridades que deberá cubrir el municipio, se identificará el impacto de las afectaciones y se proporcionarán las bases de una estrategia para la contingencia operativa.

- Medidas preventivas.

Definiremos que medidas efectivas debemos tomar para controlar los diferentes accesos a los activos computaciones, consideraremos que actividades realizar para los resguardos de la información.

- Previsión ante siniestros y desastres naturales.

Aunque un desastre natural es inevitable, si podemos estar preparados, aminorar las repercusiones y tener una pronta recuperación después del desastre. Y para definir lo verdaderamente importante se deben jerarquizar las aplicaciones.

- Respaldo y recuperación.

Después de haber desarrollado los puntos anteriores se profundizará sobre la hipótesis del siniestro y se determinará como respuesta el modo de recuperación.

Se deberá activar el presente plan de recuperación, si se presenta alguno de los escenarios mencionados al final de este documento.

La identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias permite mantener la operatividad frente a eventos críticos y minimizar el impacto negativo. Los usuarios deben ser parte integral del plan de recuperación, para evitar interrupciones, estar preparados para fallas potenciales y guiar hacia una solución.

Se considerará la finalización del plan cuando se ha resuelto satisfactoriamente la incidencia presentada, y en cuanto el funcionamiento del equipo, así como el servicio brindado por él, han vuelto a la normalidad.

Análisis y valoración de riesgos.

La pérdida total o parcial de los servicios pactados dentro del alcance del plan puede originarse por las siguientes causas:

- Delitos por computador o medios electrónicos que puedan afectar la prestación de los servicios del negocio.

- Utilización de técnicas como el acceso a los activos de información por medio de una identidad falsa, alteración de datos en forma no autorizada, negación de la ocurrencia de un acción o transacción, visualización de información no autorizada, negación del servicio y operación de las aplicaciones, obtención del acceso a la plataforma con todos los privilegios y roles que conlleven a la pérdida total o parcial de los servicios.

- Vulnerabilidades en sistemas operativos o en las aplicaciones que estén alojadas en el equipo de cómputo del municipio.

- Disminución en el rendimiento laboral de las personas a cargo de los diferentes departamentos.

- Exposición de accesos lógicos tales como puertas traseras, ataques asíncronos, fuga de datos, intercepción de líneas, apagado imprevisto de computadoras, ataques de negación de servicio, caballos de Troya, virus, gusanos, malware, ransomware y bombas lógicas que generen la pérdida total o parcial de los servicios del computador.

- Exposición de acceso físico tales como entradas no autorizadas, daño, vandalismo o robo de equipos o documentos, copia o visualización de información privada, alteración de equipos e información sensible, revelación al público de información privada, abuso de los recursos de procesamiento de datos que conlleven a la pérdida total o parcial de los servicios que brinda el municipio.

- Problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética.

- Falla en el servicio de internet por parte del proveedor.

- Problemas y exposiciones en bases de datos tales como procesamiento interno erróneo, actividad errónea de administración, corrupción de los archivos, acceso indebido a la base

de datos para modificarla, errores durante la generación y restauración de respaldos de información.

- Sabotaje de los procesos informáticos a causa de chantaje, fraude, descontentos, amenazas (acción disciplinaria o con despido), adictos o experimentación de problemas financieros o emocionales.

- Problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques externos para obtención o modificación indebida de información, inestabilidad del rendimiento del hardware o software.

- Dolo o imprudencia manifiesta por parte de personas directa o indirectamente involucrada en los procesos o servicios brindados por el municipio.

- Pérdida del hardware o software, propiedad del municipio.

- Pérdida o daño debido al cálculo o diseño erróneo del hardware y software. Falla o daño eléctrico interno.

- Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor o los medios empleados para extinguir y contener un incendio, ya sea por acción directa o indirecta, y las demoliciones que sean necesarias a consecuencia del incendio y que sean ordenadas en tal carácter por la autoridad competente.

- Combustión espontánea de algún elemento que forme parte de algún equipo de cómputo o dispositivo.

Medidas preventivas.

Normas efectivas para controlar los diferentes accesos a los activos computacionales y restringirlos en caso de que se presenten.

a) Acceso físico de personas no autorizadas.

Independientemente del área de que se trate, sólo el usuario al que fue asignado el equipo de cómputo tendrá acceso total al mismo, salvo indicación directa y explícita de su jefe inmediato.

b) Acceso a correo institucional.

El área de informática administrará las cuentas de usuario y contraseñas, previa solicitud por parte de las áreas que requieran altas, bajas o modificaciones. Al recibir el nombre de usuario y contraseña, el usuario final es y será el único responsable de salvaguardar sus datos.

c) Acceso a la Red Municipal.

Sólo el personal autorizado podrá ingresar a los servicios de la red de internet del municipio, el personal de informática es el único que realizará la configuración necesaria para tal efecto. En caso de detectar conexiones no permitidas, se procederá a bloquear el dispositivo en cuestión de forma definitiva.

d) Acceso al área de Servidores del municipio.

El personal del área de informática es el único que cuenta con el permiso para acceder a ésta área. Salvo alguna indicación por parte del personal directivo.

e) Acceso restringido a los sistemas, programas informáticos y datos.

Las áreas y departamentos del municipio cuentan con amplia información y sistemas diversos, para acceder a estos sistemas, se cuenta con credenciales de acceso, tales como

usuarios y contraseñas, esta información será accesible por el titular del área y al menos un integrante de la misma área. Serán ambos, los únicos facultados para acceder a la totalidad de información de su departamento.

f) Uso de celulares o dispositivos inalámbricos personales.

Se permitirá el ingreso de estos dispositivos al municipio con los permisos o restricciones que se determine en su oportunidad.

g) Uso de dispositivos de almacenamiento portátiles (Disco duro externo, memoria USB).

Se utilizarán preferentemente para realizar respaldos de información y de forma general no se compartirán, para evitar cualquier posible diseminación de virus o amenazas.

Respaldo y recuperación.

- La tarea más elemental e importante que será la base de cualquier solución ante desastres en el municipio es el denominado “Respaldo de información”. Esta actividad se realizará en base a las siguientes directivas:
- El usuario es el único responsable de salvaguardar su información, y deberá realizar su respaldo de información con una periodicidad semanal, quincenal o mensual.
- El respaldo de información realizado, se mantendrá en un lugar seguro y fácilmente accesible.
- Tanto el usuario, como su jefe inmediato deberán conocer la ubicación del respaldo.
- Los respaldos de información se efectuarán en dos ubicaciones:

1) Dispositivo físico, tal como un disco duro externo, cd, dvd o memoria USB.

2) Servicio en la nube, se recomienda el uso de “Microsoft OneDrive”, accesible desde la cuenta de correo institucional para todo el personal.

- Los servidores públicos podrán solicitar asesoría respecto a la creación de su respaldo de información al área de informática, misma que se otorgará oportunamente, tomando en cuenta la carga de trabajo del área.
- El resguardo del respaldo de información es responsabilidad del usuario.

El presente plan entrará en vigor a partir de su publicación en la página oficial del municipio de Juárez Hidalgo, Hidalgo.

Juárez Hidalgo, Hidalgo., agosto de 2023.