PRESIDENCIA MUNICIPAL DE TIZAYUCA, HIDALGO

PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD PARA LOS SISTEMAS INFORMÁTICOS

Municipio de Tizayuca, Hidalgo

Unidad de Innovación y Transformación Digital

Contenido

Capítulo I. Introducción

En la actualidad, las tecnologías de la información (TI) constituyen un eje esencial para asegurar la eficiencia, seguridad y transparencia en la prestación de los servicios públicos municipales. La gestión adecuada de los sistemas informáticos y de los recursos tecnológicos es indispensable para garantizar la continuidad operativa, la protección de la información institucional y el cumplimiento de las disposiciones legales en materia de acceso a la información y protección de datos personales.

En este contexto se reconoce la importancia de contar con instrumentos normativos y operativos que permitan prevenir, atender y mitigar los efectos de cualquier contingencia que ponga en riesgo la infraestructura tecnológica o la información bajo su resguardo.

Por ello, se presenta el Plan de Recuperación de Desastres y Continuidad para los Sistemas Informáticos, documento que establece las estrategias, procedimientos y acciones destinadas a asegurar la operación continua de los servicios informáticos esenciales en caso de incidentes, emergencias o desastres que afecten la infraestructura tecnológica municipal.

Capítulo II. Objetivo general

El presente documento regula de manera integral el *Plan de Recuperación de Desastres y Continuidad de Operaciones para los Sistemas Informáticos*, así como la gestión de los recursos tecnológicos públicos bajo resguardo de la Presidencia Municipal de Tizayuca, Hidalgo. Su propósito es garantizar una respuesta oportuna y eficaz ante incidentes o desastres, mediante el establecimiento de procedimientos seguros, eficientes y transparentes que aseguren la correcta administración, recuperación y resguardo de dichos recursos.

Su aplicación abarca la totalidad de los activos informáticos municipales, incluyendo servidores, redes, bases de datos, aplicaciones, servicios en línea y demás componentes tecnológicos, así como al personal de las distintas áreas administrativas y operativas que participan en la gestión, operación, soporte y disposición de los bienes informáticos y sistemas de información institucionales.

Capítulo III. Marco Legal

El presente documento se sustenta en lo dispuesto en el **Título Segundo** del *Marco Estatal de Control Interno para el Sector Público del Estado de Hidalgo*, **Capítulo I** “Estructura del Marco”, **Numeral 9** “Normas generales, principios y elementos de control interno”, **Apartado Tercero** “Actividades de control”, **Numeral 11**: *“Seleccionar y desarrollar actividades de control basadas en las Tecnologías de la Información y Comunicaciones (TIC)”*.

Asimismo, se observa lo señalado en los **Lineamientos de Control Interno de Municipio de Tizayuca Hidalgo**, en el apartado *"Diseño de la Infraestructura de las TIC"*, **3ra norma**, "El mantenimiento de la tecnología debe incluir los procedimientos de respaldo y recuperación de la información, así como la continuidad de los planes de operación, en función de los riesgos y las consecuencias de una interrupción total o parcial de los sistemas de energía, entre otros", así como del "Diseño de la administración de a Seguridad"

Capítulo IV. Análisis de Riesgos y de Impacto a los sistemas informáticos

I. Identificación de amenazas:

Consiste en reconocer todos los eventos o situaciones que podrían ocasionar una interrupción, daño o pérdida en los sistemas informáticos de la Administración Pública Municipal de Tizayuca, Hidalgo. En este caso, se consideran:

Amenaza	Impacto	Probabilidad	Criticidad
a) Ataque cibernético	Muy Alto	Alta	Muy Alta
b) Incendio, inundación o sismos	Muy Alto	Baja	Alta
c) Falla eléctrica	Muy Alto	Mediana	Media
d) Errores humanos	Alto	Alta	Alta
e) Error de Configuración	Medio	Alta	Media

a) Ataque cibernético:

Amenazas provenientes de actores maliciosos que buscan vulnerar la seguridad de la información institucional, como virus, ransomware, phishing, robo de datos o sabotaje digital.

b) Incendios, inundaciones o sismos:

Eventos naturales o accidentes que pueden dañar físicamente la infraestructura de TI, instalaciones eléctricas, redes y sistemas de respaldo, provocando pérdida total o parcial de los servicios informáticos.

c) Falla eléctrica:

Interrupciones en el suministro eléctrico que pueden ocasionar apagones, daños a los equipos de cómputo y pérdida de datos si no se cuenta con respaldo energético (UPS o plantas de emergencia).

d) Errores humanos:

Acciones no intencionadas del personal, como eliminaciones accidentales de información, configuraciones erróneas, o la desactivación involuntaria de servicios esenciales.

e) Error de configuración:

Un error de configuración en un sistema, ya sea de software, hardware o red, representa una vulnerabilidad que introduce a ataques y accesos no autorizados, pérdida de datos, interrupción de servicios.

II. Evaluación de Impacto

Una vez identificadas las amenazas, se debe determinar el grado de afectación que tendría una interrupción en los procesos institucionales, clasificando los sistemas y servicios informáticos de acuerdo con su importancia y nivel de criticidad:

Criterio de Impacto	Pregunta clave	Ejemplos
Operativo	¿Se paraliza un servicio esencial?	Nómina, Seguridad Pública
Financiero	¿Se generan pérdidas económicas o sanciones?	Multas, recargos
Reputacional	¿Afecta la confianza ciudadana?	Portal de Transparencia caído
Seguridad de la información	¿Hay riesgo de pérdida o filtración de datos?	Bases de datos personales

a) Procesos y sistemas críticos:

Aquellos cuya interrupción afectaría significativamente la prestación de trámites y servicios esenciales a la ciudadanía o al funcionamiento institucional. Por ejemplo: sistema de atención ciudadana, sistema de nómina, bases de datos de seguridad pública.

b) Procesos y sistemas importantes:

Su interrupción genera afectaciones administrativas o técnicas, pero pueden mantenerse controladas o solucionarse en un periodo razonable sin comprometer de inmediato los servicios esenciales. Ejemplos: sistemas de gestión documental, sistemas internos de reportes.

a. Procesos y sistemas secundarios:

Aquellos cuya interrupción no afecta directamente las operaciones críticas de la Administración y pueden postergarse sin repercusiones

mayores a corto plazo. Ejemplos: sistemas de consulta de estadísticas, aplicaciones de uso eventual.

Capítulo V. Estrategias de Respuesta a Emergencias

III. Protocolos ante diferentes tipos de incidentes:

a) Alertas tempranas.

Consiste en establecer mecanismos para la detección oportuna de incidentes que puedan convertirse en emergencias, en caso de identificar que se ha generado un incidente se inicia la evaluación de daños.

b) Evaluación de daños.

Una vez detectado el incidente, se debe realizar evaluación inicial inmediata con el objetivo de determinar la magnitud de la afectación, identificar los sistemas, servicios o recursos comprometidos y clasificar el evento según su gravedad. En caso de que la evaluación concluya que se enfrenta una emergencia total, será obligatorio activar de inmediato el Plan de Recuperación de Desastres.

c) Activación del Plan de Recuperación de Desastres.

Si la evaluación confirma que el incidente afecta la continuidad de los servicios críticos, se procede a activar formalmente el Plan de Recuperación de Desastres. Esto implica:

1. Notificar al Comité de Crisis de las tecnologías de la información

Comité de Crisis			
Orden	**Encargado**	**Rol**	**Condición de escalamiento**
1	Titular de la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos	Coordinador General del DRP	Falla crítica o impacto a sistemas de nivel crítico.
2	Coordinador de Infraestructura	Líder de infraestructura	Indisponibilidad de servidores, red, energía, respaldos fallo de hardware y software de equipos informáticos.
3	Coordinador de desarrollo de software	Líder de control de software	Falla de software, APIs, plataformas e integraciones

4	Coordinador de desarrollo web	Líder de control web	Falla de plataformas web, sistemas informáticos y app municipal.

2. Desplegar los procedimientos establecidos.
3. Designar responsables de cada tarea.
4. Priorizar la recuperación de los servicios más críticos.

Capítulo VI. Estrategias de continuidad para los sistemas informáticos

Para la aplicación de componentes que permita realizar un plan de continuación de labores, es necesario realizar los procedimientos para:

a) Mantener servicios mínimos y básicos operando.

b) Restaurar progresivamente los sistemas de criticidad alta o muy alta.

c) Acceder a respaldos de datos.

- Definir la frecuencia de respaldos (diario, semanal, mensual).
- Clasificar datos críticos.
- Guardar copias en sitio secundario (Discos Duros, SSD externa, USB etc.) y nube.
- Procedimientos de verificación de integridad de respaldos.

Capítulo VII. Recuperación de Infraestructura de las tecnologías de la Información

IV. Inventario de bienes informáticos (hardware) Crítico:

a) Servidores de bases de datos institucionales.

b) Servidores de aplicaciones.

c) Dispositivos de red (firewalls, switches, routers).

d) Equipos de respaldo energético (UPS, generadores).

e) Actualización anual de inventario de bienes informáticos, por parte de la Instancia Municipal encargada del Patrimonio Municipal**.**

V. Inventario de Software Crítico:

a) Sistemas Operativos de Servidores.

b) Aplicaciones de Gestión Administrativa.

c) Sistemas de Seguridad Informática.

d) Bases de Datos.

e) Sistemas de Atención Ciudadana.

f) Software de respaldo y recuperación.

Sistema	RTO	RPO	Nivel de Criticidad	Requisitos Técnicos	Estrategia de Recuperación
Sistema de Nómina	≤ 4 horas	≤ 1 hora	Crítico	Cluster activo-activo, replicación síncrona	Failover automático a sitio alterno
Bases de Datos Ciudadanas	≤ 8 horas	≤ 24 horas	Alto	Replicación asíncrona, backups horarios	Restauración desde backups en SAN/NAS
Correo Electrónico	≤ 24 horas	≤ 4 horas	Medio	Replicación diaria	Recuperación granular desde cintas/cloud
Sitio Web Municipal	≤ 1 hora	≤ 15 minutos	Crítico	CDN, balanceo de carga (Load Balancer)	Redirección a mirror site o modo estático
Sistema de Seguridad Pública	≤ 30 minutos	≤ 5 minutos	Crítico	Alta disponibilidad (HA), discos SSD en RAID 10	Switchover inmediato a nodo secundario

VI. Inventario de bienes informáticos (hardware) Crítico:

a) Servidores de bases de datos institucionales.

b) Servidores de aplicaciones.

c) Dispositivos de red (firewalls, switches, routers).

d) Equipos de respaldo energético (UPS, generadores).

e) Actualización anual de inventario de bienes informáticos, por parte de la Dirección de patrimonio

Elaboró	Revisó	Aprobó
P.L. Ariadna Natali Meneses Juárez Asistente Administrativo de la Unidad de Innovación y Transformación Digital	Tec. Javier Alazañes Sánchez Titular de la Unidad de Innovación y Transformación Digital	Ing. Gretchen Aline Atilano Moreno Presidenta Municipal Constitucional del Tizayuca, Hidalgo

Glosario de Términos

Backups: Copias de seguridad de datos, configuraciones o sistemas completos que se realizan de forma periódica para garantizar su recuperación en caso de pérdida, corrupción o daño. Los backups pueden almacenarse en medios físicos, servidores externos o servicios en la nube, y forman parte esencial de las estrategias de recuperación ante desastres.

Cibernéticos: Relativo a los sistemas informáticos, redes de comunicación y entornos digitales, así como a las amenazas y ataques que pueden producirse en dichos medios.

Cluster: Conjunto de servidores o nodos interconectados que trabajan de forma coordinada como si fueran un solo sistema, con el objetivo de mejorar el rendimiento, la disponibilidad y la tolerancia a fallos. Los clusters permiten distribuir cargas de trabajo y garantizar la continuidad operativa incluso si uno de los nodos presenta fallas.

Criticidad: Grado de importancia o impacto que presenta un sistema, servicio, proceso o recurso tecnológico en relación con la continuidad operativa de la institución.

Failover: Proceso automático o manual mediante el cual las funciones, servicios o cargas de trabajo de un sistema principal son transferidas a un sistema secundario o de respaldo, con el fin de mantener la disponibilidad del servicio en caso de falla, interrupción o mantenimiento del sistema principal.

Hardware: Componentes físicos y tangibles de un sistema informático, tales como servidores, computadoras, dispositivos de almacenamiento, routers, switches y periféricos.

Load Balancer: Dispositivo o software encargado de distribuir de manera equitativa el tráfico de red o las solicitudes de servicio entre varios servidores, con el objetivo de optimizar el rendimiento, prevenir sobrecargas y mejorar la disponibilidad del servicio.

Phishing: Técnica de fraude cibernético que utiliza comunicaciones falsas (generalmente correos electrónicos o mensajes) para engañar a los usuarios y obtener información confidencial, como contraseñas o datos bancarios.

Ransomware: Tipo de software malicioso que cifra o bloquea el acceso a la información o sistemas, exigiendo el pago de un rescate para su liberación. Representa una amenaza crítica para la disponibilidad y confidencialidad de los datos institucionales.

Redirección a mirror site: Procedimiento mediante el cual el tráfico o solicitudes de un sistema se desvían a un sitio espejo (mirror site), que es una copia exacta y sincronizada del sitio principal. Esta medida se utiliza para garantizar la continuidad de los servicios ante fallas, sobrecargas o contingencias en el sistema principal.

RPO (Recovery Point Objective – Objetivo de Punto de Recuperación): Cantidad máxima de datos que puede perderse, medida en tiempo, debido a una interrupción. Define el punto en el tiempo al que deben restaurarse los datos para reanudar las operaciones.

RTO (Recovery Time Objective – Objetivo de Tiempo de Recuperación): Periodo máximo tolerable de inactividad de un sistema, servicio o proceso crítico, medido desde el momento de la interrupción hasta su plena restauración operativa.

Sistemas de criticidad alta: Son aquellos sistemas, servicios o recursos tecnológicos cuya interrupción, degradación o falla ocasiona un impacto grave e inmediato en la continuidad operativa de la institución, comprometiendo de forma significativa la prestación de servicios públicos esenciales, la seguridad de la información o el cumplimiento de obligaciones legales y normativas.

Software: Conjunto de programas, aplicaciones y sistemas operativos que permiten el funcionamiento de los dispositivos y la ejecución de tareas específicas en un entorno informático.

Switchover: Transición planificada y controlada de las operaciones de un sistema principal hacia un sistema secundario o de respaldo, normalmente programada para realizar mantenimientos, actualizaciones o pruebas, minimizando la interrupción del servicio.

TI (Tecnologías de la Información): Conjunto de recursos, herramientas, equipos, programas, aplicaciones y procedimientos que permiten la recopilación, procesamiento, almacenamiento, gestión y transmisión de información dentro de una organización.