Mineral de la
Reforma
2024 - 2027
Ciudad de la Comunidad

Plan de Recuperación de Desastres y Continuidad de la Operación.

I. INTRODUCCIÓN

El presente documento establece el Plan de Recuperación de Desastres y Continuidad de la Operación (DRP/BCP) para los sistemas informáticos del Ayuntamiento de Mineral de la Reforma, Hidalgo. Su objetivo es garantizar:

- La continuidad operativa en caso de incidentes o desastres.
- La protección de la infraestructura tecnológica y de los datos institucionales.
- La resiliencia de los servicios municipales mediante medidas de prevención, protección y administración de riesgos.

Este plan se fundamenta en lo dispuesto por los siguientes ordenamientos jurídicos:

- Artículo 115 fracción II de la Constitución Política de los Estados Unidos Mexicanos.
- Artículo 141 fracción II de la Constitución Política del Estado de Hidalgo.
- Artículo 7 y artículo 56 fracción I inciso b) de la Ley Orgánica Municipal para el Estado de Hidalgo.
- Artículo 158 fracción I y II del Reglamento Interno de la Administración Pública Municipal de Mineral de la Reforma.

- **Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo.**

- **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.**

-

Objetivos específicos del plan:

1. **Minimizar el impacto de interrupciones no deseadas.**

2. **Definir procesos estandarizados para responder y recuperarse de incidentes.**

3. **Salvaguardar la disponibilidad, integridad y confidencialidad de la información.**

II. ALCANCE

Este plan aplica a:

1. **Servidores públicos del Ayuntamiento.**

2. **Unidades Administrativas y Áreas de Apoyo de la Administración Pública Municipal.**

3. **Proveedores y terceros con acceso a la infraestructura tecnológica municipal.**

Indicaciones:

- Todo el personal que intervenga en este plan debe conocer los lineamientos de seguridad de la información y contar con acuerdos de confidencialidad.

- Las áreas involucradas deben definir y documentar sus niveles de acceso y responsabilidades para la protección de información y la continuidad operativa.

III. INFRAESTRUCTURA CRÍTICA

1. Hardware

- **Servidor NAS de escritorio con 4 bahías, expandible a 9 bahías**
  - Revisar la temperatura interna del NAS al menos una vez por semana.
    - Temperatura promedio recomendada para discos duros: 35 °C a 45 °C.
    - Si supera los 50 °C, verificar ventilación o realizar mantenimiento.
  - Configurar un sistema RAID (por ejemplo, RAID 5 o RAID 6) para tolerancia a fallos.
  - Realizar un chequeo S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) de cada disco cada mes.

- **Equipos de respaldo UPS (Uninterruptible Power Supply)**
    - Revisar carga de baterías y autonomía del UPS cada trimestre.
    - Asegurar una capacidad mínima de 15 minutos para equipos críticos.
    - Realizar pruebas de corte de energía al menos una vez cada semestre.

- **Firewalls y dispositivos de seguridad perimetral**
    - Revisar reglas y configuraciones de seguridad cada tres meses.
    - Actualizar firmware y parches de seguridad en cuanto estén disponibles.
    - Monitorear continuamente los registros de eventos para detectar actividad anómala.

2. Software

- **Synology Drive Client** (para Windows®, Mac® y Linux®)
    - Programar respaldo incremental diario (lunes a viernes) y completo semanal (fin de semana).

- Ejecutar las copias de seguridad fuera del horario laboral para minimizar el impacto.
- Verificar integridad de los respaldos con restauraciones de prueba mensuales.

- **Sistemas institucionales del Ayuntamiento** (gestión documental y administrativa)
  - Mantenerlos actualizados con parches de seguridad.
  - Aplicar control de acceso basado en roles (RBAC).

- **Sistemas de monitoreo de redes y servidores**
  - Activar alertas automáticas por correo o SMS ante fallos o cargas inusuales.
  - Revisar reportes de rendimiento semanalmente para prevenir sobrecargas.

- **Software de recuperación ante desastres y gestión de incidentes**
  - Probar compatibilidad con la infraestructura existente y actualizar periódicamente.

- Mantener copias en un sitio alterno o en la nube para garantizar disponibilidad inmediata.

3. Oficina de soporte Técnico

- Coordina la ejecución de respaldos y pruebas de restauración.
- Supervisa cumplimiento de políticas de seguridad y notifica a Autoridades Municipales.
- Conduce la comunicación interna en caso de incidentes graves.

Indicaciones:

- Mantener un organigrama con suplentes para el Administrador de TI y el Equipo de Soporte.
- Definir un mecanismo de comunicación inmediata (teléfono, correo, mensajería) para emergencias.

4. Espacios Físicos

- **Centro de Datos Principal**
  - Temperatura recomendada: entre 18 °C y 25 °C.

- Revisar sensores de humo/incendio y sistemas de detección temprana una vez por semana.
- Limitar acceso mediante tarjetas, claves o biométricos.

- **Ubicación Alternativa**
  - Comprobar que cuente con conexión a Internet y respaldo eléctrico suficiente.
  - Realizar al menos un simulacro anual de conmutación total al sitio alterno.
  - Actualizar periódicamente el inventario de equipos instalados.

IV. PLAN DE RECUPERACIÓN DE DESASTRES

1. Estrategias de Respaldo y Restauración

1. Realizar copias de seguridad semanales con Synology Drive Client.
   - Respaldo incremental diario y completo semanal.
   - Generar reportes automáticos de ejecución y verificar su correcta finalización.
2. Mantener respaldos en ubicaciones físicas distintas.

- Almacenar al menos una copia fuera del sitio principal o en la nube.

- Documentar en una bitácora la fecha, contenido y localización de respaldos.

3. Establecer protocolos de verificación de integridad de respaldos.

   - Usar checksums o hashes para confirmar que no hay corrupción en los respaldos.

   - Realizar pruebas de restauración parciales mensuales y completas cada 6 meses.

V. MANTENIMIENTO Y ACTUALIZACIÓN DEL PLAN

1. Revisión Periódica

   - Actualizar el plan al menos una vez al año o cuando existan cambios importantes en la infraestructura.

2. Nuevas Tecnologías y Amenazas Emergentes]

   - Evaluar uso de nubes, virtualización y nuevas herramientas de ciberseguridad.

   - Monitorear amenazas (ransomware, DDoS, etc.) y reforzar protocolos.

3. **Capacitación y Concientización**

   - Realizar cursos de continuidad de operaciones y seguridad de la información.

   - Fomentar la cultura de prevención y respuesta rápida a incidentes.

4. **Control de Cambios**

   - Documentar y aprobar cualquier modificación en procedimientos e infraestructura.

   - Garantizar que todos los involucrados tengan acceso a la versión vigente del plan.

   -

VI. ACCIONES COMPLEMENTARIAS

A continuación, se detallan acciones adicionales que refuerzan y complementan la eficacia de este Plan de Recuperación de Desastres y Continuidad de la Operación:

1. **Mantenimiento Preventivo**

   - **Limpieza física de equipos** (servidores, NAS, UPS, redes) de manera trimestral.

   - Revisión de **cables y conexiones** para detectar daños o desgastes.

- Registro de **temperatura y humedad** del centro de datos al menos **dos veces al día.**

- Configuración de **alarmas automáticas** para notificar al personal en caso de desvío de valores normales de temperatura/humedad.

2. Gestión de Incidentes y Sistema de Tickets

- Implementar un **software de mesa de ayuda** (sistema de tickets) para centralizar reportes de fallas e incidentes.

- Definir **niveles de severidad** y tiempos de respuesta (SLA) en cada tipo de incidente.

- Crear un **diagrama de escalamiento** que indique a quién contactar si el incidente no se soluciona en primera instancia.

3. Pruebas de Vulnerabilidad y Penetración

- Realizar **escaneos de vulnerabilidades** al menos cada trimestre en servidores y dispositivos de red.

- Programar **pruebas de penetración** (pentesting) anuales o tras cambios importantes en la infraestructura.

- Priorizar la **remediación de vulnerabilidades** según su criticidad y verificar su corrección con nuevos escaneos.

4. Refuerzo de Ciberseguridad

- Habilitar **autenticación multifactor (MFA)** en accesos administrativos y sistemas críticos.

- Aplicar **cifrado de datos** tanto en tránsito (SSL/TLS) como en reposo (cifrado de discos) donde sea viable.

- Gestionar de manera segura las llaves de cifrado y limitar su acceso a personal autorizado.

5. Clasificación de la Información

- Definir **categorías de información** (pública, interna, confidencial).

- Identificar qué repositorios manejan datos sensibles y reforzar medidas de seguridad.

- Implementar políticas de **retención y depuración** de datos para no almacenar información innecesariamente.

6. Actualización Dinámica del Plan

- Revisar y **actualizar el plan** inmediatamente después de cada incidente real o simulacro, incorporando lecciones aprendidas.

ELABORA

JESÚS MORELOS HERNÁNDEZ
DIRECTOR DE INFORMÁTICA

REVISA

NANCY CARRILLO HERNÁNDEZ
SECRETARIA DE ADMINISTRACIÓN

Autoriza

EDUARDO MEDÉCIGO RUBIO
PRESIDENTE MUNICIPAL CONSTITUCIONAL
DE MINERAL DE LA REFORMA, HIDALGO