Tabla de contenido

1. Propósito

El propósito de este documento es establecer los lineamientos, responsabilidades y controles técnicos para la generación, custodia y prueba de las copias de seguridad (backups) de la información institucional del **H. Ayuntamiento de Morelia**.

A través de esta política, se busca garantizar la **resiliencia operativa** de la institución mediante:

- **Disponibilidad Garantizada:** Asegurar que la información crítica pueda ser recuperada en los tiempos requeridos ante fallos de hardware, errores humanos o desastres naturales.
- **Protección contra Ciberataques:** Implementar esquemas de respaldo (como la regla 3-2-1) que permitan la recuperación de datos ante incidentes de Ransomware o sabotaje.
- **Integridad de los Datos:** Validar que la información respaldada sea idéntica a la original y esté libre de corrupciones.
- **Continuidad de los Servicios Ciudadanos:** Minimizar el impacto de una pérdida de datos en la atención al público y en los procesos administrativos municipales.

2. Alcance

Esta política es de cumplimiento obligatorio para todo el personal de la Dirección de TI y aquellos enlaces técnicos responsables de la administración de sistemas en las diversas dependencias. Cubre todos los activos de información críticos, incluyendo:

2.1. Datos Estructurales y de Aplicación

- **Bases de Datos:** Sistemas de Tesorería, Catastro, Nómina y trámites ciudadanos.
- **Sistemas de Archivos:** Carpetas compartidas, documentos administrativos y expedientes digitales.
- **Configuraciones de Red:** Respaldos de las reglas de Firewall, switches y configuraciones de VPN.

2.2. Infraestructura de Servidores

- **Imágenes de Servidores (Snapshots):** Copias completas de máquinas virtuales y servidores físicos críticos para una recuperación rápida (*Bare Metal Recovery*).

2.3. Entornos de Almacenamiento

- Almacenamiento local (NAS/SAN del Ayuntamiento).
- Almacenamiento en la nube (Cloud Backup).
- Medios extraíbles autorizados para copias *Off-site*.

3. Políticas de Gestión de Copias de Seguridad

3.1. Adopción del Estándar de Resiliencia 3-2-1

El Ayuntamiento establece como norma obligatoria para toda su infraestructura crítica el esquema de respaldo **3-2-1**, asegurando la redundancia y disponibilidad de la información bajo los siguientes criterios:

- **3 Copias de los Datos:** Se mantendrá siempre el dato original y al menos dos copias adicionales de respaldo actualizadas.
- **2 Medios Distintos:** Los respaldos deben almacenarse en tecnologías de almacenamiento diferentes para evitar fallos simultáneos por degradación de hardware (ej. arreglos de discos locales y almacenamiento en nube o cinta).
- **1 Copia Fuera de Sitio (Off-site):** Es mandatorio que al menos una copia de seguridad resida en una ubicación física o lógica distinta a la del Centro de Datos principal, protegida contra desastres geográficos o eventos que afecten el edificio municipal.

3.2. Inmutabilidad y Protección contra Ransomware

Dada la criticidad de los ataques de cifrado de datos, el Ayuntamiento priorizará el uso de **Respaldos Inmutables**(tecnología WORM - *Write Once, Read Many*). Una vez generado el respaldo, este no debe permitir su modificación ni borrado por un periodo determinado, incluso si las credenciales del administrador de red se ven comprometidas.

3.3. Clasificación de Datos y Frecuencia de Respaldo

La periodicidad de las copias se define en función del **Objetivo de Punto de Recuperación (RPO)** de cada dependencia:

- **Nivel Crítico (Sistemas Financieros, Catastro, Nómina):** Respaldos incrementales diarios o en tiempo real, con respaldos completos semanales.
- **Nivel Operativo (Sistemas de Archivos, Gestión Administrativa):** Respaldos diarios al cierre de la jornada.
- **Nivel de Configuración (Configuraciones de Red y Servidores):** Respaldo tras cada cambio significativo en la arquitectura.

3.4. Cifrado y Seguridad de las Copias

- **Cifrado en Reposo:** Todos los archivos de respaldo deben estar cifrados mediante algoritmos robustos (**AES-256**o superior). Las llaves de cifrado deben ser custodiadas bajo el principio de dualidad (dos personas autorizadas) y nunca almacenarse en el mismo servidor de respaldos.
- **Control de Acceso:** El acceso a los sistemas de backup será restringido exclusivamente al personal de TI autorizado, utilizando el principio de "menor privilegio" y autenticación multi-factor (MFA).

3.5. Pruebas de Restauración y Validación de Integridad

Un respaldo que no ha sido probado no se considera válido.

- **Validación Automática:** Se deben configurar verificaciones automáticas de suma de comprobación (checksum) para asegurar que la copia no esté corrupta.
- **Ejercicios de Restauración:** La Dirección de TI deberá realizar simulacros de restauración parcial cada mes y restauraciones completas semestrales sobre entornos de prueba para validar el **Tiempo de Recuperación Objetivo (RTO)** y asegurar que el sistema puede volver a la vida en los plazos que la operación municipal requiere.

3.6. Retención y Disposición Final

- **Periodos de Retención:** Los respaldos se conservarán conforme a las obligaciones legales de transparencia y contabilidad del Estado de Michoacán. Los respaldos históricos (anuales) se mantendrán en almacenamiento frío de largo plazo.
- **Eliminación Segura:** Al cumplirse el periodo de retención, la eliminación de los soportes lógicos o físicos debe realizarse mediante métodos que garanticen la imposibilidad de recuperación de la información, generando un certificado de destrucción si aplica.

3.7. Responsabilidades de Respaldo en Entornos de Usuario

Aunque la Dirección de TI es responsable de los servidores, los usuarios son responsables de almacenar su información de trabajo en las unidades de red o nubes institucionales designadas. La política establece que **no se realizarán respaldos de información almacenada localmente** en los discos duros de las estaciones de trabajo (C:) a menos que se trate de un caso excepcional autorizado.

3.8. Uso de Medios Físicos y Almacenamiento "Cold Storage"

El Ayuntamiento reconoce el uso de **Discos Duros Externos** como un método válido y necesario para cumplir con la parte "Off-site" y "Diferente medio" de la Regla 3-2-1.

- **Aislamiento Físico (Air-Gap):** Estos medios deben permanecer desconectados de cualquier equipo o red una vez terminado el proceso de copia, funcionando como una reserva "fría" de información.
- **Cifrado Obligatorio:** Queda estrictamente prohibido realizar respaldos en discos duros externos sin el uso de cifrado de hardware o software (ej. BitLocker o VeraCrypt). Un disco perdido sin cifrar se considera una **brecha de seguridad grave**.
- **Custodia y Transporte:** Los discos que contengan respaldos institucionales deben ser transportados y almacenados en contenedores resistentes (anti-golpes e ignífugos) y bajo la supervisión directa del personal de TI designado.

4. Procedimientos

4.1. Configuración y Ejecución del Ciclo de Respaldo Local

El ciclo de protección inicia con la programación automatizada de las tareas en el software de gestión (ej. Veeam, Azure Backup, etc.). Se configuran respaldos **incrementales** diarios para ejecutarse fuera del horario laboral (ej. 22:00 hrs) para no afectar el rendimiento de los servicios ciudadanos. Los fines de semana se programará un respaldo **sintético o completo** para consolidar la cadena de datos.

El sistema debe realizar una captura de imagen de servidores críticos (Snapshots) y un volcado de bases de datos (SQL Dumps) en caliente, asegurando que la información sea consistente. Los datos resultantes se almacenan en el primer medio: un repositorio local de alta velocidad (NAS o SAN institucional) protegido con cuotas de acceso restringidas.

4.2. Sincronización y Transferencia Fuera de Sitio (Off-site)

Una vez concluido el respaldo local con éxito, el sistema dispara automáticamente la tarea de **Copia Secundaria**. Bajo la regla 3-2-1, esta copia se transfiere mediante un canal cifrado (VPN o enlace dedicado) hacia el segundo medio de almacenamiento, el cual debe estar ubicado fuera de las instalaciones principales del Ayuntamiento (ej. almacenamiento en nube institucional o un servidor espejo en una dependencia geográficamente distinta).

En caso de utilizar medios físicos (discos externos o cintas), el encargado de TI debe realizar la extracción del medio, etiquetarlo con la fecha y contenido, y transportarlo en un contenedor ignífugo y resistente a golpes hacia la bóveda de resguardo externa autorizada.

4.3. Monitoreo de Salud y Validación de Integridad

Cada mañana, durante la primera hora de operación, el administrador de TI debe revisar el **Tablero de Control de Respaldos**. El procedimiento exige verificar que todas las tareas nocturnas tengan el estado de "Exitoso".

Si se detecta un estado de "Advertencia" o "Fallo", se debe revisar el archivo de log para identificar la causa (ej. falta de espacio, pérdida de conexión o error de escritura). No se permite dejar un fallo sin atender por más de 24 horas; se debe ejecutar un respaldo manual inmediato tras corregir el error para no perder el punto de recuperación del día.

4.4. Procedimiento de Prueba de Restauración (Simulacros)

Para garantizar que los datos son recuperables, se ejecutan pruebas de restauración de la siguiente manera:

- **Prueba Mensual (Nivel Archivo):** Se selecciona una carpeta al azar de un respaldo reciente y se restaura en una ubicación temporal. Se verifica que los archivos abran correctamente y que la metadata sea íntegra.
- **Prueba Semestral (Nivel Sistema):** Se realiza una restauración completa de un servidor crítico en un entorno aislado (VLAN de pruebas). Se verifica que el sistema operativo arranque, los servicios inicien y las bases de datos sean accesibles.

Los resultados de estas pruebas, incluyendo el tiempo que tomó la recuperación (**RTO**), se registran obligatoriamente para la auditoría del SGSI.

4.5. Gestión de Inmutabilidad y Cifrado

Durante la generación de cada copia, el software debe aplicar un cifrado de grado militar (**AES-256**). Las llaves de cifrado se almacenan en un gestor de llaves independiente o en un dispositivo físico resguardado por el titular de la Dirección de TI.

Para los repositorios designados como **Inmutables**, se activa el bloqueo de retención que impide que cualquier usuario (incluso con permisos de Administrador) pueda borrar o

modificar los archivos de respaldo por un periodo de 30 días, creando una zona de seguridad impenetrable contra ataques de Ransomware que intenten destruir los backups.

4.6. Rotación y Depuración de Medios de Resguardo

Siguiendo la política de retención, el sistema de gestión de backups ejecutará una depuración automática de las copias que hayan excedido su tiempo de vida (ej. después de 12 meses para respaldos mensuales).

Si se utilizan medios físicos, se realiza una rotación semanal. El medio más antiguo en la bóveda regresa al Ayuntamiento para ser sobrescrito, mientras que el más nuevo se envía a resguardo. Antes de que un medio físico sea desechado por fin de vida útil, se procede a su desmagnetización o destrucción física, documentando el proceso en el acta de baja correspondiente.

4.7. Ejecución de Respaldo Manual en Medios Extraíbles

Para las dependencias que utilicen discos duros físicos, se seguirá la siguiente secuencia:

1. **Conexión y Montaje:** Se conecta el disco duro externo al servidor de respaldo o estación de trabajo autorizada únicamente durante la ventana de copia.
2. **Verificación de Identidad:** El sistema debe reconocer el volumen cifrado mediante la clave de acceso custodiada por el administrador.
3. **Ejecución de la Copia:** Se realiza la transferencia de los archivos o la imagen del sistema utilizando una herramienta que verifique la integridad de la copia (ej. Robocopy con verificación o software de backup especializado).
4. **Desconexión Segura:** Una vez finalizada y verificada la copia, se procede a la extracción lógica y física del disco. **Nunca debe dejarse el disco conectado** tras finalizar la tarea, para evitar que sea alcanzado por un malware en caso de infección activa.
5. **Etiquetado Físico:** El disco se etiqueta externamente con un código único, la fecha del respaldo y el nivel de clasificación de la información (ej. *BK-MORELIA-2026-01-29-CONFIDENCIAL*).
6. **Traslado a Bóveda:** El disco se coloca en su estuche de protección y se traslada a la ubicación externa (fuera del edificio municipal), registrando la salida en la **Bitácora de Movimiento de Medios (F-BC-05)**.

4.8. Rotación de Discos (Estrategia Abuelo-Padre-Hijo)

Se implementará un esquema de rotación física para maximizar la vida útil de los discos y la disponibilidad de versiones:

- **Hijo (Diario):** Se usa para las copias de lunes a jueves.
- **Padre (Semanal):** Se realiza el viernes y se lleva a la ubicación externa.
- **Abuelo (Mensual):** Un disco que se guarda permanentemente (o por un año) como cierre de mes.

5. Definiciones

- **3-2-1 (Regla de Oro):** Estrategia de respaldo que consiste en tener al menos **3** copias de los datos, en **2** tipos de soportes distintos, con **1** de ellos ubicado fuera de las instalaciones principales (Off-site).
- **Air-Gap (Brecha de Aire):** Medida de seguridad técnica que consiste en mantener un dispositivo de almacenamiento físicamente desconectado de cualquier red o sistema eléctrico cuando no está en uso, protegiéndolo de ataques lógicos como el Ransomware.
- **Cifrado (Encryption):** Proceso de transformar la información en un formato ilegible mediante un algoritmo (ej. AES-256), de modo que solo pueda ser recuperada por quienes poseen la llave de descifrado.
- **Cold Storage (Almacenamiento en Frío):** Datos almacenados en medios que no están conectados permanentemente a la red y a los que se accede con poca frecuencia, ideal para archivos históricos o de cumplimiento legal.
- **Inmutabilidad:** Atributo de un respaldo que garantiza que los datos no pueden ser modificados, sobrescritos o borrados por nadie (incluyendo administradores) durante un periodo de tiempo predefinido.
- **RPO (Recovery Point Objective - Objetivo de Punto de Recuperación):** La cantidad máxima de datos que la institución está dispuesta a perder medida en tiempo (ej. si el RPO es de 24 horas, el respaldo debe ser diario).
- **RTO (Recovery Time Objective - Objetivo de Tiempo de Recuperación):** El tiempo máximo permitido para restaurar un servicio o sistema después de un fallo antes de que el impacto sea inaceptable para la operación municipal.
- **Respaldo Incremental:** Tipo de copia que solo guarda los archivos que han cambiado desde el último respaldo realizado, optimizando el espacio y el tiempo de ejecución.

- **Respaldo Sintético / Completo:** Proceso de consolidar todas las copias incrementales en un nuevo archivo maestro que contiene la totalidad de la información actualizada.
- **WORM (Write Once, Read Many):** Tecnología de almacenamiento que permite que la información sea escrita una sola vez y leída muchas veces, impidiendo cualquier alteración posterior del registro original.

6. Formatos

Para que la operación de los respaldos sea rastreable y cumpla con el principio de responsabilidad proactiva, se establecen los siguientes registros obligatorios:

- **F-BC-01: Bitácora Diaria de Verificación de Respaldos**
  - *Uso:* Registro matutino donde el técnico confirma si las tareas programadas (locales y en nube) fueron exitosas.
- **F-BC-02: Reporte de Pruebas de Restauración y Validación**
  - *Uso:* Documento técnico que detalla el simulacro mensual/semestral, indicando qué se restauró, cuánto tiempo tomó (**RTO**) y si los datos fueron íntegros.
- **F-BC-03: Inventario y Control de Medios Físicos (Air-Gap)**
  - *Uso:* Listado de los discos duros externos, sus números de serie y la fecha de su última rotación.
- **F-BC-04: Bitácora de Movimiento de Medios y Cadena de Custodia**
  - *Uso:* Registro de quién retira el disco físico del Ayuntamiento, hacia qué ubicación externa se traslada y quién lo recibe para su resguardo.
- **F-BC-05: Acta de Baja y Destrucción de Medios de Almacenamiento**
  - *Uso:* Evidencia de que un disco duro dañado o fuera de vida útil fue destruido físicamente para evitar la recuperación de datos residuales.

7. Relación Normativa (ISO 27001:2022)

Este documento es el sustento primordial para la resiliencia del Ayuntamiento y se alinea con los siguientes controles internacionales:

Control Anexo A	Título del Control	Justificación del Cumplimiento
8.13	**Copias de seguridad de la información**	**Control Core:** Se cumple mediante la regla 3-2-1, la inmutabilidad y las pruebas de restauración.
5.30	**Preparación de las TIC para la continuidad del negocio**	Los respaldos garantizan que los servicios ciudadanos puedan restablecerse tras un desastre mayor.
8.10	**Almacenamiento de medios**	Cubre la gestión de los discos físicos, su cifrado y su resguardo en ubicaciones externas seguras.
8.1	**Dispositivos de usuario final**	Se vincula con la política de no respaldar información local (C:), obligando al uso de unidades de red.
8.7	**Protección contra malware**	El uso de respaldos inmutables y "Air-gap" es la defensa final contra ataques de Ransomware.