Tabla de contenido

1. Propósito

El presente documento tiene como objetivo establecer el marco estratégico y operativo para garantizar la **Continuidad del Negocio (BCP)** del H. Ayuntamiento de Morelia. Se busca asegurar que los procesos críticos de la institución puedan ser recuperados y mantenidos en niveles aceptables tras una interrupción significativa (desastres naturales, ataques cibernéticos, fallas de infraestructura o crisis sanitarias).

A través de esta política, se persiguen los siguientes objetivos estratégicos:

- **Resiliencia Institucional:** Garantizar que los servicios esenciales a la ciudadanía (recaudación, trámites, seguridad pública) sigan operando o se restablezcan en el menor tiempo posible.
- **Gestión del Tiempo de Recuperación:** Establecer metas claras de recuperación mediante la definición de **RTO** (Tiempo Objetivo de Recuperación) y **RPO** (Punto Objetivo de Recuperación) para cada proceso crítico.
- **Protección de la Integridad de los Datos:** Asegurar que, tras una contingencia, la pérdida de datos sea mínima y esté dentro de los límites tolerables definidos por la institución.
- **Mitigación de Impacto:** Reducir las pérdidas económicas, legales y de reputación derivadas de una interrupción prolongada de los servicios municipales.
- **Cumplimiento Normativo:** Alinearse con el control **5.29** de la **ISO 27001:2022** y las mejores prácticas de la **ISO 22301**, proporcionando evidencia auditable a través del formato **BCP**.

Agencia de la Ciudad Inteligente y Transformación Digital
H. Ayuntamiento de Morelia

2. Alcance

Esta política es de **cumplimiento obligatorio** para todas las secretarías, direcciones y departamentos del H. Ayuntamiento de Morelia que operen procesos definidos como "Críticos". El alcance del Plan de Continuidad del Negocio (BCP) comprende:

2.1. Procesos Críticos Institucionales

Aplica a todas las funciones cuya interrupción genere un impacto alto en la ciudadanía o la legalidad:

- **Sistemas de Recaudación y Tesorería:** Garantizar la disponibilidad de los portales de pago y bases de datos financieras.
- **Gestión de Trámites Ciudadanos:** Procesos de registro civil, catastro y atención pública.
- **Seguridad y Protección Civil:** Sistemas de comunicación y respuesta ante emergencias que dependen de la infraestructura de TI.
- **Nómina y Recursos Humanos:** Procesos esenciales para la operatividad interna del Ayuntamiento.

2.2. Infraestructura Tecnológica (DRP)

Cubre la recuperación de los activos críticos endurecidos mediante el proceso de Hardening:

- **Centro de Datos (SITE):** Servidores físicos y virtuales, almacenamiento y sistemas de energía ininterrumpida (UPS).
- **Conectividad:** Enlaces de internet, VPNs para trabajo remoto y redes locales (LAN) de las dependencias municipales.
- **Sistemas de Información:** Software de gestión gubernamental, bases de datos y portales web oficiales.

2.3. Capital Humano y Espacios Físicos

- **Roles Críticos:** Identificación del personal clave necesario para ejecutar el BCP (Comité de Crisis).
- **Sedes Alternas:** Espacios físicos o modalidades de teletrabajo en caso de que las oficinas principales no sean accesibles.

2.4. Dimensiones de la Recuperación

El alcance se mide a través de las métricas definidas en el formato **BCP**:

- **RTO (Recovery Time Objective):** El tiempo máximo tolerado para restablecer un servicio después de la caída.
- **RPO (Recovery Point Objective):** La cantidad máxima de datos que el Ayuntamiento está dispuesto a perder (medido en tiempo desde el último respaldo).
- **MTPD (Maximum Tolerable Period of Disruption):** El límite de tiempo antes de que la interrupción cause un daño irreversible.

3. Políticas de Continuidad del Negocio

3.1. Identificación y Clasificación de Procesos Críticos

- **Análisis de Impacto al Negocio (BIA):** Es obligatorio que cada dependencia identifique sus procesos vitales y los documente en el formato **BCP**, determinando el impacto legal, financiero y ciudadano de una interrupción.

- **Priorización de Recuperación:** Los recursos de TI se asignarán prioritariamente a los procesos con el **RTO**(Tiempo Objetivo de Recuperación) más corto, asegurando que los servicios de mayor impacto social se restablezcan primero.

3.2. Estrategia de Recuperación ante Desastres (DRP)

- **Alta Disponibilidad:** Los sistemas clasificados como "Críticos" deben contar con esquemas de redundancia y respaldos fuera de sitio (off-site), ya sea en una sede física alterna o en una nube segura, para garantizar el cumplimiento del **RPO** (Punto Objetivo de Recuperación).
- **Dependencia Tecnológica:** Todo nuevo software o infraestructura debe ser evaluado para asegurar que puede integrarse a la estrategia de continuidad existente antes de su puesta en producción.

3.3. Estructura de Respuesta y Comunicación

- **Comité de Crisis:** Se debe establecer un equipo de respuesta a emergencias con roles y responsabilidades definidos. Este comité es el único facultado para activar oficialmente el Plan de Continuidad. Este Comité estará integrado por: Titular de la Agencia de la Ciudad Inteligente y Transformación Digital, Titular de la Secretaría del Ayuntamiento, Titular de la Secretaría de Administración, Titular de la Tesorería Municipal, y, Titular del Órgano Interno de Control.
- **Directorios de Emergencia:** Se mantendrá un directorio actualizado de contactos clave (proveedores, personal crítico y autoridades) tanto en formato digital como físico, accesible fuera de la red institucional.

3.4. Ciclo de Pruebas y Simulacros

- **Ejercicios de Continuidad:** El Plan de Continuidad debe probarse al menos una vez al año mediante simulacros de escritorio o pruebas de restauración técnica para validar que el **RTO** definido en el **BCP** es alcanzable en la realidad.
- **Cultura de Prevención:** Los resultados de las pruebas deben documentarse para identificar brechas y actualizar los procedimientos, asegurando una mejora continua del sistema de gestión.

3.5. Mantenimiento del Plan

- **Actualización por Cambios:** El formato **BCP** debe actualizarse inmediatamente ante cualquier cambio significativo en la infraestructura de TI, cambios en el marco legal o reestructuraciones administrativas del Ayuntamiento.

4. Procedimientos

4.1. Desarrollo y Actualización del BCP

Este procedimiento asegura que la planificación sea precisa antes de que ocurra una crisis:

1. **Identificación de Procesos:** Cada dirección del Ayuntamiento debe listar sus actividades diarias.
2. **Análisis de Criticidad:** Se determina cuáles procesos no pueden detenerse por más de un tiempo determinado sin causar un daño grave (legal, financiero o social).
3. **Definición de Métricas en el Formato BCP:** Para cada proceso crítico, se debe asentar en el formato:
    - **RTO:** ¿En cuántas horas debemos estar operando de nuevo?
    - **RPO:** ¿A qué hora corresponde el respaldo más reciente que debemos recuperar (cuánta información podemos perder)?
    - **Responsables:** ¿Quién autoriza y quién ejecuta la recuperación?

4.2. Activación del Plan (Respuesta a Incidentes)

Cuando ocurre una interrupción significativa (falla de energía masiva, ransomware, desastre natural):

1. **Detección y Notificación:** El personal de TI detecta la falla y notifica al Comité de Crisis.
2. **Evaluación de Daños:** Se determina si la interrupción superará el tiempo de respuesta normal de soporte técnico.
3. **Declaración de Contingencia:** Si el impacto es mayor a lo tolerable, se activa formalmente el **BCP**.

4.3. Recuperación Técnica (Ejecución del DRP)

Enfoque en la infraestructura tecnológica para cumplir con el RTO/RPO:

1. **Restauración de Respaldos:** Se recuperan los datos desde el sitio de resguardo (físico o nube) asegurando que los relojes estén sincronizados para mantener la integridad.
2. **Levantamiento de Servicios:** Se activan primero los servidores y redes que soportan los procesos con el RTO más corto (ej. Tesorería antes que Archivo).
3. **Verificación de Hardening:** Se valida que los sistemas recuperados mantengan sus configuraciones de seguridad antes de abrirlos a los usuarios.

4.4. Operación en Modo de Contingencia

1. **Sedes Alternas o Teletrabajo:** Si el SITE o las oficinas no son accesibles, el personal crítico se traslada a las sedes definidas o activa la conexión vía VPN.
2. **Comunicación Institucional:** Se informa a las dependencias y, de ser necesario, a la ciudadanía sobre el estado de los servicios y los tiempos estimados de restablecimiento.

4.5. Retorno a la Normalidad (Vuelta a Casa)

1. **Sincronización de Datos:** Una vez reparada la falla primaria, se migran los datos generados durante la contingencia al sistema principal.
2. **Desactivación del BCP:** Se informa que la operación ha vuelto a su estado habitual.
3. **Análisis Post-Mortem:** Se revisa el desempeño del plan, se mide si se cumplieron los RTO/RPO y se actualiza el formato **BCP** con las lecciones aprendidas.

4.6. Programa Anual de Simulacros y Pruebas

Para garantizar que el Plan de Continuidad sea funcional y que el personal esté capacitado:

1. **Ejecución Obligatoria:** La Dirección de TI, en conjunto con el Comité de Crisis, deberá realizar al menos **un simulacro integral de continuidad al año**.
2. **Tipos de Prueba:** Se podrán alternar entre "Pruebas de Escritorio" (revisión de roles y comunicación) y "Pruebas Técnicas de Recuperación" (restauración real de sistemas críticos en entornos de prueba).
3. **Medición de Métricas:** Durante el simulacro se cronometrará el tiempo de recuperación real para compararlo contra el **RTO** estipulado en el formato **BCP**.
4. **Informe de Resultados:** Al finalizar, se emitirá un reporte detallando los éxitos y las fallas detectadas, el cual servirá como evidencia de cumplimiento ante auditorías de la **ISO 27001**.

5. Definiciones

- **BCP (Business Continuity Plan):** Plan integral que describe cómo el Ayuntamiento continuará operando durante y después de una interrupción.
- **DRP (Disaster Recovery Plan):** Componente técnico del BCP enfocado específicamente en la recuperación de la infraestructura de TI y los datos.
- **RTO (Recovery Time Objective):** El tiempo máximo permitido para que un proceso o sistema sea restablecido tras un fallo.
- **RPO (Recovery Point Objective):** La cantidad máxima de datos (expresada en tiempo) que la institución puede permitirse perder entre el último respaldo y el momento del incidente.
- **Proceso Crítico:** Aquella actividad institucional cuya interrupción por un periodo breve pone en riesgo la legalidad, las finanzas o la seguridad ciudadana de Morelia.
- **Simulacro:** Ejercicio práctico para validar la efectividad de las estrategias de recuperación y la preparación del personal.

6. Formatos

Para la gestión de la resiliencia institucional, se utilizará el siguiente formato maestro:

1. **F-CON-01: Plan de Continuidad del Negocio (BCP)**
   - **Contenido:** Identificación de procesos, análisis de impacto (BIA), definición de RTO/RPO por proceso, inventario de recursos críticos, directorio de emergencia y registro de resultados de simulacros.

7. Relación Normativa (ISO 27001:2022)

Este bloque cierra el cumplimiento de los controles de resiliencia de la norma internacional:

Control	Título	Justificación del Cumplimiento
5.29	**Continuidad de la SI durante interrupciones**	Exige la planificación para mantener la seguridad de la información durante una crisis.
5.30	**Preparación de las TIC para la continuidad**	Obliga a que la infraestructura técnica sea capaz de recuperarse en los tiempos definidos (**RTO**).

Control	Título	Justificación del Cumplimiento
8.13	**Seguridad de la red (Redundancia)**	Se vincula con la necesidad de enlaces y servidores alternos para evitar puntos únicos de falla.
Cláusula 9.2	**Auditoría interna / Pruebas**	Los simulacros anuales sirven como evidencia de que el sistema de gestión se prueba y mejora constantemente.

Agencia de la Ciudad Inteligente y Transformación Digital
H. Ayuntamiento de Morelia