Tabla de contenido

1. Propósito

El presente documento tiene como objetivo establecer los lineamientos y métodos técnicos para la eliminación y disposición segura de activos de información, soportes de almacenamiento y documentos físicos del H. Ayuntamiento de Morelia. Se busca garantizar que la información sensible sea destruida de forma irreversible, impidiendo su recuperación por personas no autorizadas una vez que el activo ha cumplido su vida útil.

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

- **Prevención de Fugas de Información:** Asegurar que los datos personales y confidenciales no sean recuperables tras la baja de equipos de cómputo, servidores o periféricos.
- **Gestión Responsable de Residuos:** Cumplir con las normativas ambientales y de disposición de residuos electrónicos (RAEE), sin comprometer la seguridad de la información.
- **Trazabilidad del Desecho:** Mantener un registro histórico que certifique que cada activo fue destruido o borrado mediante métodos validados.
- **Mitigación de Riesgos Legales:** Evitar sanciones por parte de los órganos de transparencia (IMAIP/INAI) derivadas de la mala disposición de expedientes o soportes digitales.
- **Cumplimiento Normativo:** Alinearse con el control **8.10** de la **ISO 27001:2022** referente al borrado de información y disposición de medios.

2. Alcance

Esta política es de **cumplimiento obligatorio** para todas las dependencias del H. Ayuntamiento de Morelia, proveedores de servicios de reciclaje tecnológico y personal de TI encargado del mantenimiento de activos. El alcance comprende:

H. Ayuntamiento de Morelia

2.1. Medios de Almacenamiento Digital

Aplica a todos los dispositivos internos o externos que contengan o hayan contenido datos:

- **Unidades de Disco:** Discos duros mecánicos (HDD) y unidades de estado sólido (SSD) de servidores, laptops y PCs de escritorio.
- **Dispositivos Extraíbles:** Memorias USB, tarjetas SD, discos duros externos y cintas de respaldo (LTO).
- **Memoria Volátil y Caché:** Equipos de red (routers, switches) que almacenan configuraciones sensibles.

2.2. Dispositivos y Periféricos

Aplica a la baja definitiva de hardware que procesa información:

- **Equipos Finales:** Laptops, tablets y teléfonos celulares institucionales.
- **Centros de Impresión:** Multifuncionales y fotocopiadoras (específicamente sus discos internos y memorias donde se almacenan colas de impresión).
- **Cámaras y NVRs:** Dispositivos de videovigilancia que contengan grabaciones de áreas sensibles.

2.3. Soportes Físicos (Papel)

- **Documentación Confidencial:** Expedientes ciudadanos, nóminas, contratos, planos de infraestructura y cualquier documento con datos personales protegidos por la **LGPDPPSO**.
- **Borradores y Notas:** Papelería de oficina que contenga información técnica o estratégica del Ayuntamiento.

2.4. Ciclo de Vida del Activo en Disposición

Rige durante las siguientes situaciones:

- **Obsolescencia:** Equipos que han cumplido su vida útil y serán donados o destruidos.
- **Falla Irreparable:** Dispositivos dañados que aún contienen datos en sus platos o chips de memoria.
- **Reasignación de Activos:** Antes de entregar un equipo usado a un nuevo usuario o dependencia, se debe aplicar el borrado seguro para evitar la fuga interna de información.

3. Políticas de Eliminación y Disposición Segura

3.1. Prohibición de Métodos de Borrado Estándar

- **Insuficiencia del Formateo:** Queda estrictamente prohibido el uso de formateos rápidos o la simple eliminación de particiones como método único de disposición para activos que contengan información confidencial o datos personales.
- **Borrado Lógico:** Todo borrado de software debe asegurar que los sectores del disco sean sobreescritos múltiples veces mediante algoritmos reconocidos (ej. DoD 5220.22-M).

3.2. Uso de Herramientas y Servicios Especializados

- **Uso de Software Certificado:** Para activos que serán reasignados o donados, el Ayuntamiento podrá utilizar herramientas de borrado seguro de clase mundial como **Blancco** o similares.
- **Garantía de Irreversibilidad:** El uso de estas herramientas debe garantizar que el borrado es permanente y que cumple con estándares globales de saneamiento de datos (NIST 800-88), permitiendo la reutilización segura del hardware sin rastro de información institucional.

3.3. Contratación de Terceros para Destrucción

- **Proveedores Certificados:** En caso de contratar servicios externos para la disposición de grandes volúmenes de activos (RAEE), el proveedor deberá contar con certificaciones que avalen sus procesos de destrucción de datos.
- **Cadena de Custodia:** Todo proveedor externo deberá garantizar una cadena de custodia segura desde la recolección en las instalaciones del Ayuntamiento hasta el sitio de destrucción final.
- **Derecho a Testificar:** El Ayuntamiento se reserva el derecho de supervisar físicamente el proceso de destrucción o trituración realizado por el tercero.

3.4. Destrucción Física de Medios Dañados

- **Inoperabilidad Técnica:** Si un medio de almacenamiento (HDD, SSD, Cinta) presenta fallas mecánicas que impidan el borrado por software, se debe proceder obligatoriamente a la destrucción física (trituración, perforación o desmagnetización).
- **Centros de Impresión y Copiado:** Antes de devolver o desechar multifuncionales, se debe ejecutar la función de "borrado de datos de disco" integrada en el hardware o remover físicamente la unidad de almacenamiento.

3.5. Emisión de Certificados de Destrucción

- **Evidencia Documental:** Todo proceso de eliminación, ya sea interno o a través de un tercero, debe culminar con la emisión de un **Certificado de Destrucción de Datos**.
- **Contenido del Certificado:** El documento debe incluir el ID del activo, el número de serie del componente de memoria, el método de destrucción utilizado y la firma del responsable.

3.6. Disposición de Información Física (Papel)

- **Triturado Seguro:** La documentación física clasificada como confidencial debe ser destruida mediante trituradoras de corte cruzado que impidan la reconstrucción de los documentos.
- **Prohibición de Reutilización:** Queda prohibido el uso de hojas con datos personales o información oficial para notas internas o como papel de reciclaje si el contenido es aún legible.

4. Procedimientos

4.1. Solicitud de Baja y Recolección

1. **Identificación del Activo:** El área solicitante debe generar un ticket o solicitud de baja, identificando el equipo por su número de inventario y serie.
2. **Clasificación de la Información:** La Agencia de la Ciudad Inteligente y Transformación Digital verificará si el equipo procesaba datos personales o información confidencial (ej. nóminas, registros de catastro) para determinar el nivel de borrado requerido.
3. **Resguardo Seguro:** Mientras el equipo espera su eliminación, deberá permanecer en un área restringida y bajo llave de la Dirección de Patrimonio Municipal resguardada para evitar el acceso no autorizado a los datos residuales.

H. Ayuntamiento de Morelia

4.2. Ejecución del Borrado Lógico (Software)

Para equipos de baja, reasignación u otro fin:

1. **Selección de Herramienta:** Se utilizará software certificado (como **Blancco** o herramientas de sobreescritura multinivel) para asegurar que el borrado cumpla con el estándar **NIST 800-88**.
2. **Ejecución:** Se realizará la sobreescritura de todos los sectores del disco (mínimo 3 pasadas).
3. **Verificación:** El sistema de borrado debe generar un reporte técnico que confirme que el 100% de los sectores fueron saneados con éxito.

4.3. Procedimiento para Destrucción Física

Para medios dañados o de alta criticidad:

1. **Desmontaje:** Se removerá físicamente el soporte de almacenamiento (HDD, SSD, Chips de memoria) de la carcasa del equipo.
2. **Inutilización:** Se procederá a la destrucción mecánica (perforación de platos en discos mecánicos o trituración de chips en unidades sólidas).
3. **Registro Fotográfico:** Se recomienda tomar evidencia visual del estado final del soporte de almacenamiento antes de su disposición como residuo electrónico.

4.4. Gestión con Proveedores Externos

En caso de contratar a un tercero para la disposición:

1. **Inventario de Entrega:** Se realizará un acta de entrega-recepción detallando cada unidad entregada al proveedor.
2. **Supervisión del Proceso:** Un representante de la Dirección de TI podrá acudir a las instalaciones del proveedor para atestiguar la destrucción masiva.
3. **Validación de Certificados:** Una vez concluido el proceso, el proveedor deberá entregar el **Certificado de Destrucción de Datos**, el cual será cotejado contra el inventario inicial de entrega.

4.5. Emisión del Certificado Interno y Cierre

1. **Generación de Acta:** Se llenará el formato de **Certificado de Destrucción de Datos**, anexando los reportes de software (ej. el certificado generado por Blancco) o la evidencia de destrucción física.
2. **Firma de Conformidad:** El responsable de seguridad y el técnico ejecutor firmarán el documento.
3. **Actualización de Inventario:** Se marcará el activo como "Eliminado de forma segura" en el sistema de control de activos del Ayuntamiento, resguardando la evidencia documental para auditorías de la **ISO 27001**.

5. Definiciones

- **RAEE (Residuos de Aparatos Eléctricos y Electrónicos):** Equipos de informática y telecomunicaciones que han sido desechados y requieren un manejo ambiental y de seguridad específico.

- **Saneamiento de Datos (Data Sanitization):** Proceso de hacer que el acceso a los datos en el medio sea imposible para un nivel determinado de esfuerzo, utilizando métodos como el borrado lógico, desmagnetización o destrucción física.
- **Algoritmo DoD 5220.22-M:** Estándar de sobreescritura de datos que utiliza una serie de pasadas con patrones de bits para asegurar que la información original sea irrecuperable.
- **NIST 800-88:** Guía de las mejores prácticas para el saneamiento de medios de almacenamiento, reconocida internacionalmente como el estándar de oro para el borrado seguro.
- **Certificado de Destrucción:** Documento legal y técnico que avala que la información contenida en un medio ha sido eliminada de forma irreversible.
- **Borrado Lógico Certificado:** Uso de software especializado (como Blancco) que genera evidencia auditable del proceso de saneamiento sin destruir el hardware físicamente.

6. Formatos

Para garantizar la trazabilidad y la evidencia auditable en las revisiones de seguridad, el Ayuntamiento operará bajo los siguientes formatos:

1. **F-ELI-01: Acta de Baja y Recolección de Activos de Información**
   - Utilizado para documentar el retiro de un equipo de su área operativa y su ingreso al área de resguardo seguro.
2. **F-ELI-02: Reporte Técnico de Borrado Seguro (Interno/Software)**
   - Este formato incluye los certificados generados por herramientas como Blancco para equipos que serán reasignados o donados.
3. **F-ELI-03: Certificado de Destrucción de Datos (Final)**
   - Documento maestro que consolida la evidencia de la eliminación (ya sea por software o destrucción física) y cierra el ciclo de vida del activo en el inventario.

H. Ayuntamiento de Morelia

7. Relación Normativa (ISO 27001:2022)

Este documento cumple estrictamente con los controles de protección física y lógica de la información:

Control	Título	Justificación del Cumplimiento
8.10	**Eliminación de la información**	Establece los métodos para borrar datos de manera que no puedan ser recuperados tras la baja del activo.
7.14	**Eliminación o reutilización segura de equipos**	Garantiza que el equipo se limpie de datos antes de ser desechado, vendido o reasignado.
7.10	**Almacenamiento de medios físicos**	Asegura que los discos y cintas que esperan su destrucción se mantengan en un lugar bajo llave y restringido.
5.34	**Privacidad y protección de PII**	Evita sanciones legales al impedir que datos personales de ciudadanos terminen en basureros electrónicos públicos.

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