Tabla de contenido

1. Propósito

El presente documento tiene como objetivo establecer el marco estratégico de **Prevención de Fugas de Información (DLP - Data Loss Prevention)** del H. Ayuntamiento de Morelia. Esta política no se limita al uso de herramientas tecnológicas específicas, sino que se define como la integración y ejecución armónica de un conjunto de buenas prácticas, controles físicos, lógicos y administrativos destinados a evitar la salida no autorizada de información sensible.

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

- **Enfoque en la Tríada de Seguridad:** Garantizar que la prevención de fugas sea el resultado de la correcta implementación del cifrado, el control de accesos y la disposición segura de activos.
- **Mitigación del Factor Humano:** Establecer reglas claras de conducta y manejo de información para reducir el riesgo de fugas accidentales o malintencionadas por parte del personal.
- **Protección del Patrimonio Informativo:** Blindar los datos personales de los ciudadanos y la información estratégica del Ayuntamiento mediante capas de seguridad superpuestas (Defensa en Profundidad).
- **Cultura de Responsabilidad:** Fomentar en todas las dependencias la conciencia de que la seguridad de la información es una tarea compartida que depende del cumplimiento de los procesos de acceso y resguardo.
- **Cumplimiento de la LGPDPPSO:** Asegurar que el manejo de datos personales cumpla con los principios de licitud y seguridad exigidos por la ley, evitando incidentes que comprometan la privacidad ciudadana.

2. Alcance

Esta política es de **cumplimiento obligatorio** para todo el personal (base, confianza y honorarios), prestadores de servicios profesionales, proveedores y cualquier tercero que tenga acceso a los activos de información del H. Ayuntamiento de Morelia. La prevención de fugas de información se aplica en los siguientes tres estados:

H. Ayuntamiento de Morelia

2.1. Información en Reposo (Data at Rest)

Aplica a la protección de los datos almacenados en los contenedores institucionales:

- **Servidores y Bases de Datos:** Protección de registros ciudadanos y financieros mediante el control de acceso lógico y cifrado.
- **Equipos Finales y Portátiles:** Resguardo de archivos en discos duros de laptops y PCs mediante políticas de seguridad física.
- **Soportes Físicos:** Archivos, expedientes y documentos resguardados en oficinas y el SITE.

2.2. Información en Tránsito (Data in Motion)

Aplica a la protección de los datos mientras viajan por la infraestructura:

- **Comunicaciones de Red:** Uso de protocolos seguros y cifrados para la transferencia de archivos internos.
- **Correo Electrónico:** Supervisión del uso correcto de las cuentas institucionales para el envío de información oficial.
- **Dispositivos Extraíbles:** Control y restricción del uso de memorias USB, discos externos y otros medios de almacenamiento masivo.

2.3. Información en Uso (Data in Use)

Aplica a la protección de los datos mientras el usuario interactúa con ellos:

- **Visualización en Pantalla:** Prácticas de "Escritorio Limpio y Pantalla Bloqueada" para evitar la exposición involuntaria a terceros.
- **Impresión de Documentos:** Gestión segura de los centros de impresión para evitar que documentos sensibles queden abandonados en las bandejas.
- **Manejo Humano:** Prevención de la fuga de información mediante ingeniería social o divulgación verbal no autorizada.

2.4. Integración con otros Procesos

La prevención de fugas se considera extendida y vinculada directamente con:

- **Eliminación Segura:** Garantizar que la información no se fugue al final de su ciclo de vida.
- **Gestión de Proveedores:** Asegurar que los terceros cumplan con los acuerdos de confidencialidad (NDA).
- **Control de Accesos:** Limitar la exposición de datos basándose en el principio de "necesidad de saber".

3. Políticas de Prevención de Fugas de Información (DLP Estratégico)

3.1. Protección Basada en la Clasificación de la Información

- **Etiquetado y Manejo:** Toda información identificada como "Confidencial" o "Datos Personales" debe ser manejada bajo los controles más estrictos de acceso y resguardo definidos en la **Matriz de Riesgos de Seguridad de la Información.**
- **Principio de Necesidad de Saber:** El acceso a la información se otorgará exclusivamente al personal cuya función técnica o administrativa lo requiera, evitando la sobreexposición de datos.

3.2. Controles de Salida y Medios Extraíbles

- **Restricción de Puertos USB:** Se debe limitar el uso de memorias USB y discos externos; solo se permitirán aquellos autorizados por la Dirección de TI que cuenten con cifrado de hardware si la criticidad de la información lo amerita.
- **Uso de Canales Oficiales:** Queda estrictamente prohibido el envío de información institucional, archivos de ciudadanos o bases de datos a través de correos personales, servicios de mensajería instantánea no oficiales o plataformas de almacenamiento en la nube personales.

3.3. Seguridad en la Interacción con el Usuario (Escritorio Limpio)

- **Control de Impresión:** El personal debe recoger de inmediato cualquier documento impreso con datos sensibles; no se permite dejar información abandonada en bandejas de centros de impresión o multifuncionales.
- **Bloqueo de Estaciones de Trabajo:** Es obligatorio bloquear la sesión del equipo de cómputo siempre que el usuario se retire de su lugar, impidiendo que terceros visualicen o extraigan información en su ausencia.

3.4. Cifrado como Control Transversal

- **Protección del Dato:** Toda información sensible que deba ser enviada fuera de la red municipal o almacenada en dispositivos portátiles (laptops, USB) debe estar cifrada para asegurar que, en caso de extravío o robo del medio físico, la información permanezca ilegible.

3.5. Blindaje del Final del Ciclo de Vida

- **Eliminación Obligatoria:** Ningún activo de información o soporte físico puede ser desechado sin pasar por el proceso de **Eliminación y Disposición Segura**, garantizando que la "basura tecnológica" no se convierta en una fuente de fuga de datos.

3.6. Compromiso de Confidencialidad

- **Acuerdos Jurídicos:** Todo el personal y prestadores de servicios deben tener vigente su Acuerdo de Confidencialidad (NDA); el incumplimiento de estas prácticas de prevención será sujeto a las sanciones administrativas y legales correspondientes según el marco legal aplicable.

4. Procedimientos

4.1. Verificación de Seguridad en el Puesto de Trabajo

Este procedimiento asegura que la información "en uso" no sea vulnerable:

1. **Rondas de "Escritorio Limpio":** El responsable de seguridad o TI realizará inspecciones aleatorias para verificar que no existan documentos confidenciales, post-its con contraseñas o dispositivos USB no autorizados en los lugares de trabajo.
2. **Validación de Bloqueo:** Se configurará mediante GPO (Directiva de Grupo) el bloqueo automático de sesión tras 10 minutos de inactividad, supervisando que los usuarios no deshabiliten esta función.

H. Ayuntamiento de Morelia

4.2. Control de Medios Extraíbles y Puertos

Para mitigar la fuga por hardware:

1. **Inventario de Dispositivos Autorizados:** Solo las unidades USB registradas y cifradas por la Dirección de TI podrán ser utilizadas para el movimiento de archivos institucionales.
2. **Bloqueo Lógico:** Se mantendrán deshabilitados los puertos USB para almacenamiento masivo en equipos de áreas administrativas que no justifiquen su uso, conforme al procedimiento de **Hardening**.
3. La habilitación de los puertos USB será bajo la estricta autorización de las instancias correspondientes y los procedimientos diseñados para tal fin.

4.3. Supervisión de Canales de Salida (Correo y Red)

1. **Monitoreo de Archivos Adjuntos:** Se realizarán revisiones periódicas de los logs de tráfico de correo institucional para identificar envíos inusuales de archivos de gran tamaño o bases de datos a dominios externos no gubernamentales.
2. **Cifrado de Comunicaciones:** Todo envío de información clasificada como "Confidencial" fuera de la red municipal debe seguir el procedimiento de cifrado antes de ser transmitido.

4.4. Auditoría de Impresión y Desecho

1. **Purga de Colas de Impresión:** Semanalmente se revisarán los registros de los centros de impresión para asegurar que no existan trabajos acumulados que contengan datos sensibles.
2. **Validación de Destrucción:** Cualquier documento impreso que deba ser desechado debe pasar inmediatamente por la trituradora de corte cruzado, siguiendo la política de **Eliminación y Disposición Segura**.

4.5. Gestión de Incidentes de Fuga

En caso de detectar una salida no autorizada de información:

1. **Contención:** Se procederá al bloqueo inmediato del acceso del usuario involucrado y a la revocación de permisos en la red.
2. **Documentación:** Se abrirá el **Formato de Registro de Incidentes** para detallar qué información salió, por qué medio y el impacto potencial.
3. **Análisis Forense:** Se revisarán los registros de acceso lógico y físico para determinar la trazabilidad del evento y fortalecer los controles preventivos.

5. Definiciones

- **DLP (Data Loss Prevention):** Conjunto de estrategias y controles destinados a garantizar que los datos sensibles no se pierdan, se utilicen mal o se acceda a ellos por parte de usuarios no autorizados.
- **Información en Reposo:** Datos que se encuentran almacenados de forma persistente en dispositivos (discos duros, bases de datos, nubes).

- **Información en Tránsito:** Datos que se están moviendo a través de una red, ya sea interna o hacia el exterior (correos, transferencias web).
- **Información en Uso:** Datos con los que el usuario está interactuando activamente (abiertos en pantalla, impresos o en memoria RAM).
- **Ingeniería Social:** Técnicas de manipulación psicológica utilizadas para conseguir que los usuarios revelen información confidencial o cometan errores en la seguridad.
- **Escritorio Limpio:** Práctica de seguridad que exige que la información sensible (papeles, USB, notas) sea retirada del puesto de trabajo cuando este no se encuentra bajo supervisión.

6. Formatos

Para que la prevención sea medible y auditable, nos apoyaremos en los formatos transversales ya establecidos, evitando la duplicidad administrativa:

1. **F-MON-05: Bitácora de Accesos Físicos y Digitales**
   - *Uso:* Verificar quién accedió a la información antes de una fuga sospechada.
2. **F-MON-01: Formato de Registro de Incidentes**
   - *Uso:* Documentar cualquier evento donde se confirme o sospeche de la salida no autorizada de datos.
3. **F-HAR-01: Registro de Hardening de Activos**
   - *Uso:* Evidencia de que los puertos USB y servicios de salida están bloqueados o restringidos en los equipos.
4. **Acuerdo de Confidencialidad (NDA) para Empleados y Terceros**
   - *Uso:* Sustento legal para la responsabilidad individual del manejo de la información.

7. Relación Normativa (ISO 27001:2022)

Esta política de "DLP por buenas prácticas" cumple con los siguientes controles de la norma internacional:

Control	Título	Justificación del Cumplimiento
8.12	**Prevención de fuga de datos**	Se cumple mediante la aplicación de medidas técnicas y administrativas para detectar y prevenir la extracción de información.

Control	Título	Justificación del Cumplimiento
7.15	**Política de escritorio limpio y pantalla limpia**	Mitiga la fuga de información en el estado de "Información en Uso" dentro de las oficinas del Ayuntamiento.
8.1	**Dispositivos de usuario final**	Asegura que laptops y móviles no sean puntos de fuga mediante el bloqueo de puertos y configuraciones seguras.
5.12	**Clasificación de la información**	Es la base del DLP: no se puede prevenir la fuga de lo que no se ha identificado como sensible.

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