Tabla de contenido

1. Propósito

El presente documento tiene como objetivo establecer los lineamientos estratégicos y técnicos para el uso de mecanismos de **cifrado, criptografía y enmascaramiento de datos** dentro del H. Ayuntamiento de Morelia. El fin primordial es asegurar la confidencialidad, integridad y autenticidad de la información institucional y de los datos

personales de la ciudadanía, protegiéndolos contra accesos no autorizados, alteraciones o filtraciones.

A través de esta política, se busca alcanzar los siguientes objetivos:

- **Protección del Dato en sus Tres Estados:** Garantizar que la información esté protegida cuando está almacenada (**en reposo**), cuando viaja por la red (**en tránsito**) y cuando es procesada por aplicaciones o personal administrativo (**en uso**).
- **Gestión Centralizada y Técnica:** Operativizar el uso de herramientas criptográficas mediante la **Matriz Criptográfica**, asegurando que todos los sistemas utilicen algoritmos robustos y actualizados, evitando el uso de métodos obsoletos o vulnerables.
- **Cumplimiento Legal y de Privacidad:** Alinearse con la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados*, utilizando el enmascaramiento para que el personal administrativo solo tenga acceso a la información mínima necesaria para cumplir sus funciones (Principio de Necesidad de Saber).
- **Gobernanza de Llaves Criptográficas:** Definir un marco seguro para la generación, almacenamiento, rotación y destrucción de llaves, entendiendo que la seguridad del cifrado reside totalmente en la protección de la llave.
- **Mitigación de Impacto por Robo o Extravío:** Asegurar que, ante la pérdida física de dispositivos móviles o medios de almacenamiento, la información permanezca inaccesible para terceros mediante el cifrado de disco completo.

H. Ayuntamiento de Morelia

2. Alcance

Esta política es de cumplimiento obligatorio para la Dirección de TI, desarrolladores de software, administradores de bases de datos y cualquier tercero con acceso a la infraestructura del Ayuntamiento. El alcance se divide en los siguientes dominios:

2.1. Alcance sobre los Datos (Clasificación)

La aplicación de controles criptográficos y de enmascaramiento se rige por la sensibilidad de la información:

- **Datos Personales y Sensibles:** Toda información que permita identificar a un ciudadano o empleado (CURP, RFC, domicilio, datos biométricos).

- **Información Financiera:** Datos relativos a la recaudación de impuestos, cuentas bancarias institucionales, presupuestos y nómina.
- **Credenciales de Acceso:** Contraseñas, llaves API, tokens de sesión y certificados digitales.
- **Puertos de conexión:** Los puertos de acceso a servidores deben ser diferentes a los tradicionales.

2.2. Alcance Tecnológico (Infraestructura)

Los controles definidos en este documento y detallados en la **Matriz Criptográfica** aplican a:

- **Almacenamiento (Dato en Reposo):** Discos duros de servidores, bases de datos (SQL/NoSQL), respaldos en cinta o disco, y servicios de almacenamiento en la nube (Cloud Storage).
- **Comunicaciones (Dato en Tránsito):** Enlaces VPN, tráfico web institucional (HTTPS), protocolos de transferencia de archivos (SFTP) y comunicaciones entre aplicaciones (Web Services/APIs).
- **Dispositivos de Usuario Final:** Laptops institucionales, unidades de almacenamiento extraíble (USB/Discos externos) y dispositivos móviles enrolados.

2.3. Alcance Operativo (Procesos)

- **Ciclo de Vida de las Llaves:** Desde la generación y distribución hasta la rotación, almacenamiento seguro y destrucción de llaves criptográficas.
- **Ambientes de Desarrollo y Pruebas:** Aplicación obligatoria de **enmascaramiento de datos** en entornos que no sean de producción, asegurando que los desarrolladores trabajen con datos realistas pero no reales.
- **Desarrollo de Software Interno:** Todo código fuente generado por el Ayuntamiento que maneje funciones de cifrado o almacenamiento de datos sensibles.

2.4. Alcance sobre Terceros

Cualquier proveedor de servicios (Nube, Software as a Service o soporte externo) que procese datos del Ayuntamiento debe demostrar el uso de estándares criptográficos alineados o superiores a los establecidos en esta política.

3. Políticas de Cifrado, Criptografía y Enmascaramiento

3.1. Estándares de Algoritmos y Robustez Criptográfica

El Ayuntamiento prohíbe el uso de algoritmos de cifrado obsoletos o que hayan demostrado vulnerabilidades (como MD5 o SHA-1 para integridad).

- **Matriz Criptográfica como Referencia:** Todo sistema institucional que procese información clasificada como "Interna" o "Confidencial" debe estar registrado en la **Matriz Criptográfica**. Cualquier cambio en el algoritmo o herramienta debe actualizarse en dicha matriz de forma inmediata.
- **Nivel de Robustez:** Se establece como estándar mínimo el uso de algoritmos de cifrado simétrico **AES-256** y algoritmos asimétricos **RSA** (mínimo 2048 bits, recomendado 4096 bits) o Criptografía de Curva Elíptica (**ECC**), los sistemas que usen SHA1 O MD5, se deben actualizar.

3.2. Protección del Dato en Reposo (At Rest)

Todo almacenamiento masivo de información debe contar con una capa de cifrado activa.

- **Cifrado de Discos y Endpoints:** Todas las computadoras portátiles y medios extraíbles (USB/Discos externos) propiedad del Ayuntamiento deben utilizar cifrado de disco completo (Full Disk Encryption - FDE) mediante herramientas como BitLocker o similares. Solo en el caso de las Dependencias y entidades que cuenten con Active Directory.
- **Bases de Datos:** Las bases de datos que contengan información ciudadana (Tesorería, Catastro, Registro Civil) deben implementar Cifrado de Datos Transparente (TDE) o cifrado a nivel de columna para campos altamente sensibles.

3.3. Protección del Dato en Tránsito (In Transit)

Es obligatorio que cualquier intercambio de información a través de redes públicas o internas esté protegido.

- **Comunicaciones Web:** Todos los portales del Ayuntamiento deben utilizar certificados **TLS 1.2 o superior**(HTTPS). Se prohíbe el uso de SSL en cualquier versión y TLS 1.0/1.1.
- **Transferencia de Archivos:** Se prohíbe el uso de FTP plano. Es mandatorio el uso de protocolos cifrados como **SFTP** o **HTTPS**.

- **Administración Remota:** Todo acceso técnico a servidores o equipos de red debe realizarse mediante **SSH v2** o túneles VPN cifrados.
- **Seguridad en Redes Inalámbricas (Wi-Fi):** Se establece como requisito mínimo de seguridad el uso del protocolo **WPA2 (AES)** para cualquier punto de acceso institucional. Queda estrictamente prohibido el uso de protocolos obsoletos como WEP o WPA original. En nuevas implementaciones o renovaciones tecnológicas, se priorizará el salto a **WPA3**.
- **Autenticación en Wi-Fi:** Para redes administrativas, es obligatorio el uso de WPA2-Enterprise, vinculando el acceso a las credenciales individuales de los colaboradores.

3.4. Gestión de Llaves Criptográficas (Key Management)

La seguridad del cifrado depende totalmente de la gestión de las llaves.

- **Custodia Segura:** Las llaves privadas y certificados deben almacenarse en contenedores seguros (Key Vaults) o Módulos de Seguridad de Hardware (HSM) si la criticidad lo amerita. Queda prohibido almacenar llaves en texto plano en el código fuente o en archivos compartidos.
- **Ciclo de Vida:** Se deben establecer periodos de rotación de llaves conforme a la **Matriz Criptográfica**. En caso de sospecha de compromiso de una llave, se debe proceder a su revocación y sustitución inmediata bajo el procedimiento de gestión de incidentes.

H. Ayuntamiento de Morelia

3.5. Enmascaramiento de Datos (Data Masking)

Para cumplir con el principio de "Privacidad desde el Diseño", el Ayuntamiento aplicará técnicas de enmascaramiento:

- **Enmascaramiento Estático (Ambientes de Desarrollo):** Antes de clonar una base de datos de producción hacia ambientes de desarrollo o pruebas, se deben anonimizar o enmascarar los datos personales (ej. reemplazar nombres reales por nombres ficticios, ocultar dígitos de cuentas bancarias).
- **Enmascaramiento Dinámico (En Uso):** Los sistemas de atención ciudadana solo mostrarán los datos necesarios para la operación. Por ejemplo, en una pantalla de consulta, el personal solo podrá ver los últimos 4 dígitos de un número de identificación o cuenta, a menos que su rol requiera la visualización completa.

3.6. Uso de Firma Electrónica y Autenticidad

El Ayuntamiento fomentará el uso de firmas electrónicas avanzadas para garantizar el **No Repudio** en actos administrativos y trámites ciudadanos, asegurando que la identidad del emisor y la integridad del documento sean verificables criptográficamente.

4. Procedimientos

4.1. Mantenimiento y Evolución de la Matriz Criptográfica

La **Matriz Criptográfica (M-CR-01)** es el corazón de este control. Su gestión seguirá este flujo:

1. **Inventario de Activos Cifrados:** Por cada nuevo sistema, base de datos o servicio de red, el responsable de TI debe registrar:
    - **Algoritmo y Modo:** (Ej. AES-256 en modo GCM).
    - **Función:** (Ej. Cifrado de base de datos de Catastro).
    - **Herramienta:** (Ej. Microsoft TDE, OpenSSL).
    - **Estado del Dato:** (Reposo, Tránsito o Uso).
2. **Evaluación de Obsolescencia:** Trimestralmente, el Oficial de Seguridad revisará boletines de seguridad (NIST, OWASP) para verificar si algún algoritmo en la matriz ha sido vulnerado o degradado. De ser así, se iniciará un **Plan de Migración Criptográfica** inmediato.
3. **Control de Versiones:** La matriz debe reflejar la fecha de la última rotación de llaves para cada activo listado.

H. Ayuntamiento de Morelia

4.2. Implementación de Cifrado en Dispositivos (Endpoints y Medios)

Para garantizar que una laptop perdida en una oficina municipal no sea una brecha de datos:

1. **Aprovisionamiento de BitLocker/FDE:** Antes de entregar cualquier equipo, se debe activar el Cifrado de Disco Completo (FDE). Se configurará un PIN de pre-arranque si el dispositivo maneja información "Altamente Confidencial".
2. **Custodia de Llaves de Recuperación:** Las llaves de recuperación (48 dígitos) no se guardarán en archivos locales. Se enviarán automáticamente al Directorio Activo o a un Gestor de Secretos centralizado.

3. **Cifrado de Medios Extraíbles:** Mediante política de grupo (GPO), se forzará a que cualquier USB conectada a un equipo del Ayuntamiento sea cifrada antes de permitir la escritura de datos (BitLocker To Go).

4.3. Ciclo de Vida de Llaves Criptográficas (Key Management)

Este procedimiento asegura que las llaves no vivan para siempre ni caigan en manos equivocadas:

1. **Generación Segura:** Las llaves deben generarse en dispositivos con generadores de números aleatorios certificados (FIPS 140-2). Queda prohibido el uso de llaves generadas por scripts manuales o herramientas web no verificadas.
2. **Almacenamiento y Acceso:** Las llaves nunca deben "viajar" por correo o chats. Se almacenarán en un **Vault** (Bóveda Digital) donde el acceso sea nominal y quede registrado en un log de auditoría.
3. **Rotación Programada:** Según la criticidad definida en la Matriz Criptográfica, las llaves se rotarán:
    - **Certificados TLS/SSL:** Anualmente.
    - **Llaves Maestras de BD:** Cada 2 años.
    - **Llaves de Acceso API:** Cada 6 meses.
4. **Revocación y Destrucción:** En caso de baja de un administrador de TI o sospecha de compromiso, la llave se revoca en los registros (CRL) y se destruye el contenedor original para evitar recuperaciones forenses.

H. Ayuntamiento de Morelia

4.4. Ejecución del Enmascaramiento para Desarrollo y Pruebas

Como consultor con fondo en software, este paso es vital para tus proyectos en el Ayuntamiento:

1. **Clasificación de Campos:** El DBA identificará columnas con PII (Datos de Identificación Personal) como Nombres, RFC, CURP y Domicilios.
2. **Selección de Técnica:**
    - **Sustitución:** Cambiar "Juan Pérez" por un nombre aleatorio de una lista ficticia.
    - **Barajado (Shuffling):** Mezclar los valores de la columna para que no correspondan al registro original.
    - **Nulificación:** Poner en "nulo" campos que no se requieren para la prueba (ej. salarios).

3. **Validación de Salida:** Se realizará una prueba de "re-identificación". Si es posible adivinar quién es el ciudadano cruzando los datos enmascarados, el proceso debe repetirse con mayor agresividad.

4.5. Auditoría de Protocolos de Comunicación (WPA2/TLS)

Para asegurar que las comunicaciones no bajen la guardia:

1. **Escaneo de Red Wi-Fi:** Mensualmente se auditarán los Access Points del Ayuntamiento. Cualquier SSID que utilice WEP o WPA1 será desactivado inmediatamente. Se verificará que el estándar mínimo sea **WPA2-AES** y se escanearán de manera aleatoria los equipos de cómputo para verificar las redes almacenadas e identificar conexiones no autorizadas.
2. **Verificación de Cipher Suites en Servidores:** Se utilizarán herramientas (como SSL Labs o escaneos internos) para asegurar que los servidores web del Ayuntamiento rechacen conexiones de navegadores antiguos que pidan SSLv3 o TLS 1.0/1.1.
3. **Cifrado de Correo:** Se configurará el protocolo **TLS forzado** entre los servidores de correo del Ayuntamiento y sus principales contrapartes para asegurar que los mensajes no viajen en texto plano por el internet público.

5. Definiciones

- **AES-256 (Advanced Encryption Standard):** Algoritmo de cifrado simétrico por bloques, adoptado como estándar por el gobierno de EE. UU. y utilizado globalmente para proteger información clasificada debido a su resistencia contra ataques de fuerza bruta.
- **Criptografía Asimétrica (Llave Pública):** Sistema que utiliza un par de llaves (pública y privada). Lo que se cifra con la pública solo puede descifrarse con la privada, garantizando confidencialidad y autenticidad (ej. RSA, ECC).
- **Enmascaramiento de Datos (Data Masking):** Proceso de crear una versión estructuralmente similar pero no identificable de los datos de la organización, permitiendo su uso en entornos de baja seguridad como desarrollo o capacitación.
- **FIPS 140-2:** Estándar federal de procesamiento de información de EE. UU. que especifica los requisitos de seguridad para los módulos criptográficos.

- **HSM (Hardware Security Module):** Dispositivo físico de alta seguridad que gestiona, procesa y almacena llaves criptográficas dentro de un entorno blindado a prueba de manipulaciones.
- **No Repudio:** Capacidad de garantizar que el emisor de un mensaje no pueda negar haberlo enviado, ni el receptor haberlo recibido, gracias al uso de firmas digitales y marcas de tiempo.
- **PII (Personally Identifiable Information):** Cualquier dato que pueda ser utilizado para identificar a una persona específica (Nombre, CURP, RFC, Biométricos), los cuales son el objetivo principal del enmascaramiento.
- **TLS (Transport Layer Security):** Protocolo sucesor de SSL que asegura las comunicaciones en una red, proporcionando privacidad e integridad de los datos entre dos aplicaciones (ej. un navegador y un servidor web).

6. Formatos

Para que el control criptográfico no sea "letra muerta", el Ayuntamiento debe implementar y custodiar los siguientes registros:

- **M-CR-01: Matriz Criptográfica Institucional**
  - *Contenido:* Inventario de sistemas, bases de datos y equipos; algoritmos aplicados; fecha de última rotación de llaves; y responsable técnico.
- **F-CR-02: Registro de Entrega y Cifrado de Dispositivo Final**
  - *Contenido:* Confirmación de activación de FDE (BitLocker), ID de la llave de recuperación resguardado y firma de conformidad del usuario.
- **F-CR-03: Acta de Generación / Destrucción de Llaves Maestras**
  - *Contenido:* Documento que avala la creación o eliminación de llaves críticas bajo el esquema de "dos personas" (control dual) para evitar abusos de poder.
- **F-CR-04: Certificado de Enmascaramiento para Entornos de Desarrollo**
  - *Contenido:* Validación firmada por el DBA de que la base de datos entregada a los programadores ha sido anonimizada y no contiene datos reales de ciudadanos.

H. Ayuntamiento de Morelia

7. Relación Normativa (ISO 27001:2022)

Este documento es el sustento técnico para los siguientes controles de la norma internacional:

Control Anexo A	Título del Control	Justificación del Cumplimiento
8.24	**Uso de Criptografía**	**Control Principal:** Establece las reglas de uso, algoritmos y gestión de llaves mediante la Matriz M-CR-01.
8.11	**Enmascaramiento de Datos**	Define los procedimientos para proteger la PII en entornos no productivos y pantallas de usuario.
8.1	**Dispositivos de Usuario Final**	Garantiza que las laptops del Ayuntamiento tengan cifrado activo para mitigar el impacto por pérdida física.
8.3	**Gestión de Derechos de Acceso**	Se vincula con el acceso a las llaves criptográficas solo para personal autorizado.
8.20	**Seguridad en Redes**	Asegura que el tráfico Wi-Fi y cableado utilice protocolos de cifrado mínimos como WPA2 y TLS 1.2.

H. Ayuntamiento de Morelia