Tabla de contenido

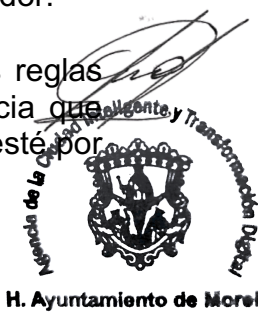
1. Propósito

El presente documento tiene como objetivo establecer los lineamientos de seguridad, responsabilidades y controles técnicos que deben observar los colaboradores del **H. Ayuntamiento de Morelia** al hacer uso de dispositivos móviles (institucionales o personales) y al realizar actividades bajo la modalidad de teletrabajo o trabajo remoto.

Con este propósito, buscamos blindar la información municipal ante los riesgos inherentes a la movilidad, enfocándonos en:

- **Protección de la Información en Tránsito:** Garantizar que cualquier dato que viaje fuera de la red física del Ayuntamiento (vía internet o redes celulares) lo haga de forma cifrada y segura, mitigando el riesgo de interceptación.
- **Regulación del BYOD (Bring Your Own Device):** Establecer los límites de uso, privacidad y seguridad cuando un colaborador utiliza sus propios dispositivos (smartphones, laptops, tabletas) para acceder a recursos institucionales, asegurando que el dispositivo personal no se convierta en una puerta trasera para ataques.
- **Control del Perímetro Lógico:** Extender los controles de seguridad de la oficina (como el MFA y el Antivirus) a cualquier ubicación remota, asegurando que el teletrabajo no signifique una relajación de las normas de seguridad.
- **Prevención de Pérdida o Robo:** Definir los mecanismos de respuesta inmediata ante el extravío de dispositivos que contengan o tengan acceso a información sensible, permitiendo el bloqueo o borrado remoto de los datos institucionales.
- **Cumplimiento del Marco Jurídico:** Asegurar que el trabajo remoto se realice bajo estándares que respeten la Ley de Protección de Datos Personales y la normativa interna del Ayuntamiento, protegiendo tanto a la institución como al colaborador.

Nota de visión: Este propósito actúa como un "escudo preventivo". Al dejar las reglas claras desde ahora, el Ayuntamiento estará preparado para cualquier contingencia que obligue al personal a trabajar a distancia, garantizando que la operatividad nunca esté por encima de la seguridad.



2. Alcance

La presente política es de observancia general para todo el personal del **H. Ayuntamiento de Morelia** que, previa autorización de su titular, realice sus funciones fuera de las instalaciones físicas de la dependencia, ya sea de forma regular o excepcional.

2.1. Modalidades de Conectividad

El alcance distingue entre dos esquemas operativos para efectos de seguridad y administración:

- **Teletrabajo Institucional:** Aplicable al personal que, bajo convenio formal, realiza sus actividades de forma permanente o híbrida (más del 40% de su jornada) fuera de las oficinas, utilizando infraestructura institucional.
- **Trabajo Remoto y Operación de Campo:** Aplicable al personal que requiere acceso a sistemas de forma esporádica o itinerante (comisiones, supervisiones de obra, inspecciones, o guardias fuera de horario), utilizando dispositivos móviles.

2.2. Categorización de Dispositivos

La política regula dos tipos de activos tecnológicos:

1. **Dispositivos Institucionales:** Laptops, tablets y smartphones propiedad del Ayuntamiento, asignados bajo resguardo al colaborador.
2. **Dispositivos Personales (BYOD - Bring Your Own Device):** Equipos propiedad del trabajador que, por necesidad del servicio y con autorización previa, se utilicen para acceder a recursos institucionales (correo, sistemas o documentos).

2.3. Ámbito de Aplicación Técnica

Este alcance cubre la seguridad de la información independientemente del medio de conexión utilizado:

- Redes domésticas (Wi-Fi privado).
- Redes públicas (Hotspots en plazas o comercios, cuyo uso se desaconseja).
- Redes de datos móviles (3G/4G/5G).
- Túneles de conexión segura (VPN).

3. Políticas de Dispositivos Móviles y Trabajo Remoto

3.1. Vinculación y Gestión Institucional Obligatoria

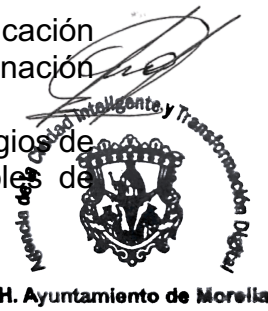
Para garantizar el control sobre la superficie de ataque, se establece que **ningún dispositivo** (laptop, tableta o smartphone) podrá acceder a la infraestructura lógica del Ayuntamiento de forma remota sin estar plenamente vinculado a un sistema de gestión centralizado.

- **Requisito de Enrolamiento:** Todo equipo debe estar enrolado en al menos una de las plataformas de gestión autorizadas: **Active Directory (AD)** para equipos Windows, o un sistema de **Gestión de Dispositivos Móviles (MDM/MAM)** para dispositivos móviles y esquemas BYOD.
- **Identificación del Activo:** El sistema de gestión debe permitir la identificación unívoca del número de patrimonio del equipo (o número de serie en BYOD) y su vinculación directa con la identidad (cuenta de usuario) del colaborador responsable.

3.2. Certificación de Aptitud mediante Hardening Obligatorio

El proceso de **Hardening (Endurecimiento de Sistema)** se define como el requisito habilitador para la operación remota. Un dispositivo solo será catalogado como "Apto" si cumple con los siguientes controles de configuración estricta:

- **Cifrado de Almacenamiento:** Es mandatorio el cifrado total de la unidad de disco (BitLocker, FileVault o equivalente) con custodia de llaves de recuperación por parte del área de TI.
- **Deshabilitación de Servicios Vulnerables:** Bloqueo de puertos de comunicación innecesarios, servicios de compartición de archivos no institucionales y eliminación de cuentas de invitado.
- **Restricción de Privilegios Locales:** El usuario final no deberá poseer privilegios de administrador en el equipo remoto para evitar la desactivación de controles de seguridad o la instalación de software no autorizado.



3.3. Conectividad Segura y Exclusividad de VPN

- **Obligatoriedad del Túnel Cifrado:** Se establece que la **Red Privada Virtual (VPN)** es el **único canal autorizado** para el acceso a servidores de archivos, bases de datos y sistemas de gestión institucional. Queda estrictamente prohibido el acceso a estos recursos mediante conexiones directas a internet o redes sin cifrar.
- **Estándares de Cifrado y MFA:** Las conexiones VPN deben emplear algoritmos de cifrado robustos (AES-256 o superior) y su establecimiento está condicionado de forma innegociable a la validación mediante **Autenticación Multi-Factor (MFA)**.
- **Prohibición de Redes Públicas:** Se prohíbe el uso de redes Wi-Fi abiertas para el ejercicio de funciones institucionales. En caso de no contar con una red privada segura, se deberá utilizar el anclaje a datos móviles (Hotspot) del dispositivo personal o institucional.

3.4. Seguridad del Punto Final (Endpoint) y Monitoreo de Postura

- **Agente de Protección Activo:** Es obligatorio que todo dispositivo cuente con el agente de seguridad (**Bitdefender** o solución endpoint institucional) activo, actualizado y reportando en tiempo real a la consola central.
- **Validación de Postura (Compliance):** El sistema de acceso lógico verificará la "salud" del equipo antes de conceder la conexión VPN. Si se detecta que el antivirus está desactivado, el firewall local está abajo o existen parches críticos de seguridad pendientes, el acceso será **denegado automáticamente**.

3.5. Regulación de Dispositivos Personales (BYOD)

- **Contenedores de Información:** En dispositivos personales, la información institucional debe residir exclusivamente dentro de aplicaciones gestionadas o "contenedores seguros" que aíslen los datos gubernamentales de la vida privada del colaborador.
- **Derecho de Borrado Selectivo:** Al utilizar un dispositivo personal, el colaborador acepta que el Ayuntamiento tiene la facultad de ejecutar un borrado remoto de la información y aplicaciones institucionales en caso de robo, pérdida o cese de la relación laboral, sin afectar los datos personales del usuario.
- **Instalación de software propiedad del Ayuntamiento en dispositivos personales:** en el marco de la Normativa de la Propiedad Industrial podrá realizarse en condiciones específicas con clara justificación.

3.6. Diferenciación Operativa y Legal (NOM-037)

- **Límites de Jornada Fuera de Oficina:** Para evitar contingencias legales, se define como **Trabajo Remoto u Operación de Campo** a toda actividad que no exceda el **40% de la jornada laboral mensual** fuera de las instalaciones.
- **Formalización de Teletrabajo:** Cualquier función que requiera superar dicho porcentaje deberá ser reportada a Recursos Humanos para la formalización del contrato de Teletrabajo, asegurando el cumplimiento de la NOM-037 y las obligaciones de seguridad asociadas.

3.7. Responsabilidades de Seguridad en el Entorno Físico Remoto

- **Privacidad del Perímetro:** El colaborador es responsable de asegurar que la pantalla y los documentos físicos no sean visibles para terceros no autorizados en su ubicación remota.
- **Reporte de Incidentes:** Ante cualquier sospecha de compromiso de seguridad, robo o extravío, el usuario debe notificar a la Dirección de TI en un periodo **menor a 2 horas**, permitiendo la revocación inmediata de certificados y el bloqueo de accesos lógicos.

4. Procedimientos

4.1. Procedimiento de Hardening y Certificación de Aptitud Técnica

Antes de que un dispositivo sea autorizado para el trabajo fuera de las instalaciones, el personal técnico de la dependencia deberá ejecutar obligatoriamente los siguientes pasos de endurecimiento:

1. **Saneamiento de Software:** Eliminación de aplicaciones no institucionales, servicios de compartición de archivos (tipo P2P) y deshabilitación de protocolos de comunicación obsoletos (ej. SMBv1).
2. **Configuración de Cuentas:** Deshabilitar la cuenta de "Invitado", renombrar la cuenta de "Administrador" local y asegurar que el colaborador opere bajo un perfil de "Usuario Estándar".
3. **Activación de Cifrado de Unidad:** Configurar e iniciar el cifrado total del disco duro mediante **BitLocker**(Windows) o **FileVault** (macOS). La clave de recuperación debe ser exportada y resguardada en el repositorio seguro de la Dirección de TI.
4. **Actualización de Seguridad:** Validar que el Sistema Operativo cuente con el último "Service Pack" o parche de seguridad crítico instalado.
5. **Verificación de Firewall:** Configurar el Firewall local para bloquear todas las conexiones entrantes no solicitadas.

4.2. Procedimiento de Vinculación (Binding) al Ecosistema Institucional

Una vez endurecido el equipo, se procederá a su integración en las plataformas de gestión:

1. **Unión al Dominio:** Para equipos Windows institucionales, se realizará la unión al **Active Directory** para la recepción automática de GPOs (Políticas de Grupo).
2. **Instalación del Agente Endpoint:** Se instalará el agente de protección de punto final (**Bitdefender** o similar), verificando que el equipo aparezca con estado "Protegido" en la consola central.
3. **Registro en el Inventario de Acceso Remoto:** Se asignará el ID del dispositivo al perfil del usuario en el sistema de gestión de accesos, vinculando la identidad del colaborador con el hardware específico.

4.3. Procedimiento de Conexión Segura con Verificación de Postura

El flujo de acceso remoto no será automático y dependerá de la validación de seguridad en tiempo real:

1. **Solicitud de Túnel:** El usuario inicia el cliente de **VPN** institucional e ingresa sus credenciales únicas.
2. **Chequeo de Postura (Health Check):** El servidor de acceso consultará automáticamente al agente del dispositivo. Si el equipo no cumple con los criterios (ej. antivirus desactivado o cifrado apagado), la conexión será rechazada y el usuario recibirá una notificación de incumplimiento técnico.
3. **Autenticación de Segundo Factor (MFA):** Superada la prueba de postura, el sistema enviará un desafío de **MFA** al dispositivo móvil vinculado del usuario.
4. **Establecimiento del Canal:** Una vez aprobado el MFA, se establece el túnel cifrado AES-256 para el tráfico de datos.

H. Ayuntamiento de Morelia

4.4. Procedimiento para el Esquema BYOD (Dispositivos Personales)

Para colaboradores autorizados a usar sus propios equipos, el procedimiento se limita a la gestión de aplicaciones:

1. **Enrolamiento de Aplicación (MAM):** El usuario instalará un perfil de gestión de aplicaciones institucionales que crea un contenedor cifrado e independiente de sus datos personales.
2. **Configuración de PIN de Contenedor:** Se obligará al uso de un PIN o biometría exclusivo para abrir las apps del Ayuntamiento (Outlook, Teams, etc.).
3. **Restricción de Copiado:** Se configurará el contenedor para impedir el "Copiar/Pegar" de información institucional hacia aplicaciones personales (como WhatsApp o redes sociales).

4.5. Procedimiento de Monitoreo y Auditoría de Dispositivos

1. **Escaneo de Vulnerabilidades:** La consola central realizará escaneos semanales de forma remota para identificar nuevas vulnerabilidades en los equipos vinculados.
2. **Reporte de Inactividad:** Mensualmente, se generará un reporte de dispositivos que no han reportado a la consola en más de 15 días; estos equipos serán marcados como "En Riesgo" y sus certificados VPN serán suspendidos temporalmente hasta su validación física.

4.6. Procedimiento ante Robo, Extravío o Compromiso de Seguridad

Ante la pérdida de un dispositivo con acceso institucional, se activará la "Ruta Crítica de Bloqueo":

1. **Notificación de Emergencia:** El usuario reporta el incidente a la Dirección de TI vía telefónica o correo alterno (tiempo máximo: 2 horas).
2. **Ejecución de Comando de Borrado (Remote Wipe):**
   - Para **Equipos Institucionales**: Se envía la señal de borrado total de disco o bloqueo de arranque.
   - Para **Equipos BYOD**: Se envía la señal de borrado selectivo, eliminando únicamente el contenedor de datos institucionales.
3. **Revocación de Credenciales:** Inhabilitación inmediata de la cuenta en Active Directory y revocación de certificados digitales de la VPN.

5. Definiciones

- **AES-256 (Advanced Encryption Standard):** Algoritmo de cifrado de bloque utilizado para proteger datos electrónicos, considerado el estándar de oro para la seguridad gubernamental.
- **BYOD (Bring Your Own Device):** Práctica donde los colaboradores utilizan sus dispositivos personales (laptops, celulares) para acceder a recursos institucionales.
- **Cifrado de Unidad (Full Disk Encryption):** Tecnología de seguridad que protege los datos mediante la conversión de la información del disco duro en código ilegible, el cual solo se descifra con la clave correcta.
- **Hardening (Endurecimiento de Sistema):** Proceso técnico de asegurar un sistema operativo mediante la reducción de su superficie de vulnerabilidad, eliminando software, servicios y privilegios innecesarios.

- **MDM / MAM (Mobile Device / Application Management):** Herramientas de software que permiten a los administradores de TI supervisar, gestionar y asegurar dispositivos móviles o aplicaciones específicas en el entorno laboral.
- **NOM-037-STPS-2023:** Norma Oficial Mexicana que establece las condiciones de seguridad y salud en el trabajo bajo la modalidad de teletrabajo.
- **VPN (Virtual Private Network):** Tecnología que crea un túnel cifrado sobre una red pública (internet), permitiendo que un dispositivo remoto se conecte a la red privada del Ayuntamiento como si estuviera físicamente ahí.

6. Formatos

Para que la gestión sea auditable y sencilla de implementar en las dependencias, utilizaremos los siguientes formatos:

- **F-DM-01: Solicitud y Autorización de Trabajo Remoto / Campo**
  - *Uso:* Registro de la necesidad operativa y validación de que el tiempo de trabajo fuera de oficina no exceda los límites legales.
- **F-DM-02: Carta Responsiva para Dispositivos Personales (BYOD)**
  - *Uso:* Documento donde el colaborador acepta la instalación del contenedor de seguridad y otorga permiso para el borrado remoto selectivo de datos institucionales.
- **F-DM-03: Lista de Verificación (Checklist) de Hardening y Certificación de Aptitud**
  - *Uso:* Hoja técnica que firma el responsable de TI tras validar que el equipo tiene cifrado, antivirus y parches al día.
- **F-DM-04: Reporte de Incidente o Robo de Equipo en Movilidad**
  - *Uso:* Activación inmediata del protocolo de bloqueo y evidencia para el proceso legal de baja patrimonial.

7. Relación con Requisitos Normativos (ISO 27001:2022)

Este mapeo asegura que cada esfuerzo técnico en Morelia esté alineado con el estándar internacional:

Control Anexo A	Nombre del Control	Descripción del Cumplimiento
5.14	**Seguridad de la información en el trabajo remoto**	Se cumple al establecer la obligatoriedad de la VPN, el MFA y las reglas de privacidad del entorno físico en casa o campo.
8.1	**Dispositivos de usuario final**	Se materializa con el proceso de **Hardening obligatorio** y la gestión mediante agentes de Endpoint (Bitdefender).
8.7	**Protección contra el malware**	Se garantiza mediante la vinculación obligatoria del dispositivo a la consola central de seguridad antes de permitir la conexión.
8.24	**Uso de criptografía**	Cumplido mediante la exigencia de cifrado de disco completo y túneles VPN con protocolos AES-256.
5.1	**Políticas para la seguridad de la información**	Este documento constituye la base normativa para la movilidad y el uso de dispositivos en el Ayuntamiento.

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