Tabla de contenido

1. Propósito

El propósito de este documento es establecer las directrices y controles necesarios para gestionar, monitorear y restringir el acceso físico a las instalaciones, oficinas y áreas sensibles del **H. Ayuntamiento de Morelia**.

Buscamos crear una cultura de "perímetro seguro" que cumpla con los siguientes objetivos estratégicos:

- **Salvaguarda de la Integridad Física:** Proteger la integridad de los colaboradores, ciudadanos y visitantes que se encuentran dentro de los inmuebles municipales.
- **Protección de Activos Críticos:** Prevenir el acceso no autorizado, daño, robo o interferencia a los activos de procesamiento de información (como el **SITE principal**, centros de datos y archivos físicos) que soportan la operación del Ayuntamiento.
- **Control de Zonas Sensibles:** Diferenciar claramente entre las áreas de atención al público y las áreas restringidas de operación interna, asegurando que solo el personal autorizado tenga acceso a estas últimas.
- **Trazabilidad de Movimientos:** Garantizar que exista evidencia auditable de quién, cuándo y con qué motivo ingresó a áreas críticas, permitiendo una respuesta efectiva ante incidentes de seguridad o pérdida de activos.
- **Cumplimiento del Marco Legal:** Alinear la gestión de accesos con la norma **ISO 27001:2022** y las disposiciones locales en materia de protección civil y resguardo patrimonial.

2. Alcance

El cumplimiento de estas directrices es obligatorio para todas las personas que requieran ingresar, permanecer o circular dentro de los inmuebles y áreas bajo la administración del **H. Ayuntamiento de Morelia**.

2.1. Ámbito Espacial (Instalaciones)

La política cubre la seguridad física de:

- **Edificios Administrativos:** Oficinas generales, palacio municipal y dependencias externas.
- **Áreas de Infraestructura Crítica:** El SITE principal (Centro de Datos), cuartos de comunicación (IDFs), áreas de plantas de emergencia y sites secundarios.
- **Áreas de Resguardo de Información:** Archivo municipal, concentrado de archivos de las dependencias y almacenes de activos tecnológicos.
- **Áreas Perimetrales:** Estacionamientos institucionales, accesos vehiculares y áreas de carga/descarga.

2.2. Ámbito Humano (Sujetos)

Este control aplica sin excepción a:

- **Servidores Públicos:** Personal de base, confianza, honorarios y funcionarios de alto nivel.
- **Visitantes:** Ciudadanos que acuden a realizar trámites o gestiones.
- **Personal de Seguridad:** Policía municipal y guardias de seguridad privada que custodian los accesos.
- **Terceros y Proveedores:** Personal de mantenimiento, soporte técnico externo, servicios de limpieza y contratistas.

2.3. Flexibilidad por Criticidad

Dada la diversidad de funciones y recursos entre las dependencias, el alcance de los controles específicos se determinará bajo un esquema de **Niveles de Seguridad**:

1. **Nivel 1 (Acceso Público):** Áreas de atención ciudadana y pasillos generales donde el control es visual o mediante CCTV.
2. **Nivel 2 (Acceso Administrativo):** Oficinas internas donde se requiere identificación institucional y el acceso está limitado a colaboradores del área.
3. **Nivel 3 (Acceso Restringido/Crítico):** Áreas como el SITE, Tesorería o Archivo, donde se exigen controles estrictos (bitácoras, llaves físicas custodiadas o biometría) y el acceso es exclusivo para personal autorizado.

3. Políticas de Gestión de Accesos Físicos

3.1. Definición de Perímetros y Niveles de Acceso

- **Zonificación de Seguridad:** Cada dependencia deberá clasificar sus espacios en al menos tres niveles (Público, Administrativo y Restringido). El nivel de control debe ser proporcional a la sensibilidad de la información que se resguarda en dicha área.
- **Barreras Físicas:** Las áreas donde se procese información sensible deben estar protegidas por barreras físicas (muros, puertas con cerradura, mamparas) que impidan el acceso no autorizado o la observación fortuita de datos.

3.2. Mecanismos de Autenticación

- **Diversidad de Controles:** Se autoriza el uso de cualquier mecanismo que garantice la identidad de quien accede, pudiendo ser:
  - **Controles Físicos:** Llaves tradicionales con control de duplicados.
  - **Controles Electrónicos:** Tarjetas de proximidad, códigos numéricos o tokens.

- **Controles Biométricos:** Huella digital, reconocimiento facial o de iris.
- **Controles Administrativos:** El acceso de los Servidores Públicos a su área de trabajo deberá ser portando su Credencial Institucional vigente, en caso de no contar con ella realizar registro en bitácoras custodiadas por personal de recepción o seguridad.

- **Gestión de Llaves y Credenciales:** Todo medio de acceso (llave, tarjeta o código) es personal e intransferible. Su pérdida debe reportarse de inmediato para la cancelación de accesos o el cambio de guardas/chapas.

3.3. Control de Visitantes y Personal Externo

- **Identificación Obligatoria:** Todo visitante debe registrar su entrada y salida. Se debe capturar, al menos, nombre, dependencia a visitar y motivo.
- **Acompañamiento Permanente:** Queda estrictamente prohibido que los visitantes transiten solos por las áreas administrativas o restringidas. **Todo visitante debe estar acompañado en todo momento** por un colaborador responsable de la dependencia durante su estancia.
- **Distintivos:** Según la capacidad de la dependencia, se podrá implementar el uso de gafetes de "Visitante" para facilitar su identificación visual dentro de las instalaciones.

3.4. Áreas Críticas (SITE y Archivos)

- **Acceso de Último Recurso:** El acceso a los centros de datos (SITE), cuartos de comunicación y archivos concentradores debe estar restringido al mínimo personal necesario.
- **Registro de Actividad:** Es obligatorio que todo ingreso a estas áreas quede asentado en una bitácora (física o digital), especificando la hora de entrada, salida y las actividades realizadas.
- **Custodia de Llaves Críticas:** Las llaves físicas de SITE o plantas de emergencia deben estar bajo resguardo de la Coordinación Administrativa o la Dirección de Infraestructura, con un protocolo claro de entrega-recepción.

3.5. Videovigilancia y Monitoreo

- **Uso de CCTV:** En dependencias donde se cuente con sistemas de videovigilancia, estos se consideran controles compensatorios que refuerzan la seguridad física. Las grabaciones deben ser tratadas con confidencialidad y conforme a las leyes de protección de datos personales.

4. Procedimientos

Para asegurar que todas las dependencias cumplan con la política independientemente de su capacidad técnica, se establecen los siguientes métodos operativos:

4.1. Gestión Integral de Visitantes y Terceros REDEFINIR

Para mitigar riesgos de ingeniería social o acceso accidental a datos sensibles, se establece lo siguiente:

1. **Protocolo de Recepción:** Al llegar, la visitante entrega una identificación (INE, Licencia, Pasaporte) que se queda bajo resguardo del área de acceso a cambio de un gafete de identificación (si la dependencia cuenta con ellos).
2. **Registro de Equipos Externos:** Si el visitante introduce laptops o medios de almacenamiento, estos deben quedar registrados en la bitácora (Marca/Serie) para evitar la extracción no autorizada de activos del Ayuntamiento al salir.
3. **Acompañamiento "Punto a Punto":** El anfitrión es responsable del visitante desde la recepción hasta su salida. Esto incluye el acompañamiento a áreas comunes (sanitarios, cafetería) si estas se encuentran dentro del perímetro administrativo. **Nunca se debe dejar a un visitante solo en una oficina con equipos encendidos o documentos expuestos.**

4.2. Control y Custodia de Medios de Acceso Físico

Dado que las llaves y credenciales son la "primera línea", su control debe ser riguroso:

1. **Inventario de Llaves:** Cada dependencia mantendrá un **Maestro de Llaves** donde se identifique qué chapa abre cada llave y quién posee copias.
2. **Protocolo de Pérdida:** Ante el extravío de una llave de un área de Nivel 3 (SITE/Tesorería), el procedimiento obligatorio es el **cambio inmediato de la guarda o cerradura**, no solo la reposición de la llave.
3. **Prohibición de Duplicados Externos:** Queda prohibido que cualquier colaborador realice duplicados de llaves institucionales en establecimientos externos sin un oficio de autorización de la Coordinación Administrativa.

4.3. Operación de Videovigilancia (CCTV) y Disuasión

Para que el CCTV sea un control efectivo y no solo un "adorno":

1. **Señalética Disuasiva:** Los letreros mencionados deben ser colocados a la **altura de la vista** en los puntos de entrada. El texto debe ser claro y en cumplimiento con la Ley de Transparencia y Acceso a la Información Pública.
2. **Verificación de Grabación:** El responsable técnico de la dependencia deberá realizar una prueba semanal para asegurar que las cámaras no solo "se vean", sino que estén **almacenando video** correctamente.
3. **Retención de Imágenes:** Se recomienda un periodo mínimo de almacenamiento de **15 a 30 días** (dependiendo de la capacidad de almacenamiento de la dependencia) para permitir investigaciones posts-incidentes.

4.4. Acceso Fuera de Horario Laboral y Días Inhábiles

Para el personal que requiera ingresar en fines de semana o noches:

1. **Autorización Previa:** Se debe contar con un permiso firmado por el titular de la dependencia enviado al área de seguridad/guardia.
2. **Registro Especial:** El guardia de turno deberá asentar en bitácora no solo la entrada, sino el motivo extraordinario de la presencia del colaborador.

4.5. Procedimiento de "Escritorio Limpio" (Vertiente Física)

Como parte del control de acceso físico, al final de la jornada:

1. **Resguardo de Información:** Todo expediente físico con datos personales o sensibles debe quedar guardado en archiveros bajo llave.
2. **Información sensible a la vista:** todo servidor público deberá abstenerse de colocar anotaciones de usuarios y contraseñas de acceso a sus cuentas a la vista.
3. **Cierre de Perímetro:** El último colaborador en salir de una oficina es responsable de verificar que ventanas estén cerradas y puertas con llave, activando alarmas si existen.
4. **Bloqueo de equipo:** el Servidor Público al ausentarse de su lugar deberá bloquear el equipo de cómputo que tenga en uso, mismo que deberá contar con contraseña o código de acceso para su desbloqueo.

4.6. Mantenimiento de Infraestructura de Seguridad

1. **Revisión de Perímetros:** Trimestralmente se deben inspeccionar puertas, ventanas, techos y muros en busca de debilidades (chapas flojas, cristales dañados, áreas de posible escalamiento).

2. **Iluminación de Seguridad:** Se debe garantizar que los puntos de acceso y áreas donde existan cámaras cuenten con iluminación suficiente durante la noche para permitir la identificación de rostros en el video.

5. Definiciones

- **Área Restringida (Nivel 3):** Espacio físico que alberga activos críticos de información (como el SITE, Tesorería o Archivo Histórico) y que requiere un control de acceso específico y registro obligatorio.
- **Aviso de Privacidad:** Documento legal que informa a los ciudadanos y colaboradores sobre el tratamiento de sus datos personales (incluyendo su imagen captada por CCTV), cumpliendo con la Ley de Protección de Datos Personales.
- **Biometría:** Método de autenticación basado en características físicas únicas del individuo (huella, rostro, iris) utilizado para permitir o denegar el acceso a sistemas o áreas físicas.
- **Bitácora de Acceso:** Registro cronológico (en papel o digital) donde se asientan las entradas y salidas de personas a una instalación o área específica.
- **CCTV (Circuito Cerrado de Televisión):** Sistema de videovigilancia compuesto por cámaras y grabadores destinados a supervisar actividades en perímetros definidos.
- **Control Compensatorio:** Medida de seguridad alternativa (como un guardia o una bitácora) que se implementa cuando no es posible o costeable instalar un control tecnológico (como un lector biométrico).
- **SITE (Centro de Datos):** Espacio físico dedicado a albergar los servidores, equipos de red y almacenamiento de datos del Ayuntamiento.

6. Formatos

Para dar cumplimiento a la política, se establecen los siguientes formatos base. Estos pueden ser adaptados a sistemas digitales siempre que conserven los campos obligatorios:

- **F-AF-01: Registro General de Visitantes y Proveedores**
  - *Campos mínimos:* Fecha, Nombre, Identificación, Empresa/Dependencia, Motivo, Hora de entrada, Firma de anfitrión (acompañante) y Hora de salida.
- **F-AF-02: Bitácora de Acceso a Áreas Críticas (SITE / Archivos)**
  - *Campos mínimos:* Nombre del técnico, Motivo del acceso (mantenimiento/revisión), Hora de entrada/salida y observaciones sobre el estado del área al finalizar.
- **F-AF-03: Control de Entrega-Recepción de Llaves y Dispositivos de Acceso**

- *Uso:* Registro de quién posee copias de llaves físicas o tarjetas electrónicas, con fecha de entrega y devolución.

- **F-AF-04: Inventario de Cerraduras y Videovigilancia**
  - *Uso:* Documento para el levantamiento trimestral del estado físico de chapas, cámaras y señalética de la dependencia.

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

En esta tabla se mapea cómo los procedimientos del Ayuntamiento de Morelia cumplen con los controles del **Anexo A** de la norma internacional:

Control Anexo A	Nombre del Control	Descripción del Cumplimiento
7.1	**Perímetros de seguridad física**	Se cumple mediante la zonificación (Niveles 1, 2 y 3) y el uso de barreras físicas según la criticidad de la dependencia.
7.2	**Controles físicos de entrada**	Implementado a través del registro obligatorio de visitantes y el uso de mecanismos de autenticación (llaves, biométricos o bitácoras).
7.3	**Seguridad de oficinas, salas y facilidades**	Se aborda en la política de "Escritorio Limpio" y el resguardo de expedientes bajo llave al finalizar la jornada.
7.4	**Monitoreo de seguridad física**	Se garantiza mediante el uso de CCTV, el mantenimiento de cámaras y la colocación de señalética de advertencia.
7.10	**Medios de almacenamiento**	El acceso restringido a archivos y SITE asegura que los medios físicos de datos no sean manipulados o extraídos sin autorización.
5.34	**Privacidad y protección de PII**	Se cumple mediante el uso de Avisos de Privacidad en las zonas monitoreadas por cámaras.

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