Tabla de contenido

1. Propósito

El propósito de este documento es establecer las directrices, controles y mecanismos de supervisión para la gestión de identidades y el control de acceso lógico a los sistemas, aplicaciones, bases de datos y redes del **H. Ayuntamiento de Morelia**.

Con esta política, se busca garantizar que el acceso a la información institucional sea concedido únicamente a los usuarios autorizados, bajo los siguientes pilares:

- **Principio de Menor Privilegio:** Asegurar que cada colaborador tenga acceso estrictamente a la información y herramientas necesarias para el desempeño de sus funciones, ni más ni menos.

- **Confidencialidad e Integridad:** Prevenir el acceso no autorizado a datos sensibles (como nóminas, registros ciudadanos o trámites de tesorería) y evitar modificaciones accidentales o malintencionadas.
- **Trazabilidad y Responsabilidad:** Establecer mecanismos para identificar de forma unívoca qué usuario realizó qué acción dentro de los sistemas, permitiendo deslindar responsabilidades en caso de incidentes.
- **Gestión del Ciclo de Vida del Usuario:** Definir un proceso estandarizado para la creación (altas), modificación (cambios de puesto) y revocación (bajas) de accesos, evitando la existencia de "cuentas huérfanas" de ex-colaboradores.
- **Estandarización Operativa:** Homologar los criterios de seguridad (como la complejidad de contraseñas) entre las dependencias que utilizan Active Directory y aquellas que gestionan accesos de forma local o en la nube.

2. Alcance

La presente política es de cumplimiento obligatorio para todo el personal que requiera interactuar con los activos de información lógicos del **H. Ayuntamiento de Morelia**, independientemente de su ubicación física o el dispositivo utilizado.

2.1. Ámbito Humano

El alcance incluye a:

- **Usuarios Internos:** Personal de base, confianza, mandos medios y superiores de todas las dependencias.
- **Usuarios Externos:** Consultores, proveedores de soporte técnico, auditores y prestadores de servicios que requieran acceso temporal o permanente a la red o sistemas institucionales.
- **Administradores de Sistemas:** Personal técnico con privilegios elevados en servidores, redes o bases de datos.

2.2. Ámbito Tecnológico (Sistemas y Plataformas)

La gestión de accesos lógicos comprende:

- **Infraestructura de Red:** Acceso a la red institucional (LAN/Wi-Fi), servicios de Directorio Activo (AD) y conexiones remotas (VPN).

- **Sistemas de Gestión Institucional:** Software de Tesorería, Catastro, , Nómina y cualquier sistema o aplicación desarrollada a medida o adquirida por las dependencias.
- **Herramientas de Colaboración:** Cuentas de correo electrónico institucional, almacenamiento en la nube (OneDrive, Google Drive), y herramientas de comunicación (Teams, Zoom).
- **Equipos de Cómputo Finales:** El inicio de sesión local en estaciones de trabajo, laptops y tabletas propiedad del Ayuntamiento.

2.3. Flexibilidad Operativa

Reconociendo la heterogeneidad tecnológica del Ayuntamiento, el alcance se adapta a dos modalidades de cumplimiento:

1. **Sistemas Centralizados (Nivel Estándar):** Aquellos integrados al **Windows Active Directory**, donde las políticas de contraseñas y sesiones se gestionan de forma masiva por la Dirección de Infraestructura.
2. **Sistemas Locales o Aislados (Nivel Autónomo):** Aquellas dependencias o sistemas que no están unidos al dominio. En estos casos, el alcance obliga a los responsables del área a implementar controles manuales que emulen los estándares institucionales (gestión de cuentas local, bitácoras de alta/baja y políticas de contraseñas manuales).

3. Políticas de Gestión de Accesos Lógicos

3.1. Identificación y Autenticación de Usuarios

- **Identificación Unívoca:** Todo usuario debe poseer un identificador único. Prohibido el uso de cuentas genéricas.
- **Secreto de Autenticación (Contraseñas):** Longitud mínima de 10 caracteres, combinando mayúsculas, minúsculas, números y símbolos.
- **MFA Obligatorio:** Se establece la **Autenticación Multi-Factor (MFA) como requisito obligatorio** para el acceso a cualquier sistema institucional, correo electrónico y conexión remota.
    - *Flexibilidad:* El método de MFA podrá ser: Aplicaciones de autenticación (OTP), tokens físicos, biometría vinculada al dispositivo, o códigos vía correo/SMS, según la capacidad técnica de la dependencia.

3.2. Gestión del Ciclo de Vida de la Cuenta

- **Formalización de Accesos:** Ningún acceso será concedido sin una solicitud formal y la autorización del titular del área, a través de Cartas Responsivas.
- **Revocación Inmediata (Bajas):** Al término de la relación laboral, los accesos deben ser inhabilitados de forma inmediata (en un plazo no mayor a 24 horas). Es responsabilidad de Recursos Humanos notificar a los administradores de sistemas sobre cualquier baja o cambio de puesto.
- **Revisión Periódica:** Los titulares de cada dependencia deben revisar semestralmente el listado de usuarios con acceso a sus sistemas para identificar y depurar cuentas inactivas o con privilegios excesivos.

3.3. Control de Privilegios (Acceso Basado en Roles)

- **Principio de Menor Privilegio:** Los accesos se otorgarán basándose estrictamente en las funciones del puesto (Role-Based Access Control). Un usuario solo debe ver y editar lo que su trabajo requiere.
- **Segregación de Funciones:** Se debe evitar que una misma persona tenga acceso a todas las etapas de un proceso crítico (ej. quien captura la nómina no debe ser la misma persona que la autoriza y dispersa en el sistema).
- **Cuentas de Administrador:** El uso de privilegios elevados (administrador de dominio, root, admin de base de datos) debe estar restringido exclusivamente al personal técnico autorizado y no debe usarse para tareas cotidianas como navegación web o lectura de correo.

H. Ayuntamiento de Morelia

3.4. Protección de Sesiones y Equipos

- **Bloqueo Automático:** Todo equipo de cómputo debe configurarse para bloquear la sesión tras un periodo de inactividad (10 minutos).
- **Control de Intentos Fallidos:** Los sistemas deben bloquear la cuenta de usuario tras un número definido de intentos de inicio de sesión fallidos para prevenir ataques de fuerza bruta.
- **Sincronización de Relojes:** Para garantizar la validez de las bitácoras (logs), todos los sistemas deben estar sincronizados con una fuente de tiempo confiable (NTP institucional).

3.5. Acceso de Terceros y Proveedores

- **Acceso Temporal:** Los proveedores externos recibirán cuentas con una vigencia limitada y privilegios restringidos al área técnica que les corresponde.
- **Supervisión Obligatoria:** Todo acceso lógico de un tercero a sistemas críticos debe ser supervisado por un responsable del Ayuntamiento y quedar registrado en bitácora.

4. Procedimientos

4.1. Procedimiento de Alta y Provisión de Accesos

1. **Solicitud:** El jefe inmediato envía el **Formato F-AL-01** a la Dirección de IT o al Administrador Local.
2. **Verificación de Identidad:** Se debe validar que el colaborador ya cuente con su **Carta de Resguardo de Activos** firmada. **NOTA: no se usa carta de resguardo, sino cartas responsivas**
3. **Configuración de Perfil:** Se asignan permisos basados en el rol (RBAC). No se otorgan permisos "por si acaso"; solo lo necesario.
4. **Enrolamiento de MFA:** En el primer inicio de sesión, el sistema debe obligar al usuario a configurar su segundo factor de autenticación. El soporte técnico asistirá en la elección del método más apto para el equipo del usuario.

H. Ayuntamiento de Morelia

4.2. Gestión de Contraseñas y Credenciales (El "Autoservicio")

Para evitar cuellos de botella administrativos, se establecen dos rutas:

- **Ruta A (Dominio):** Los usuarios en Active Directory utilizarán el portal de autoservicio para restablecer contraseñas mediante validación por MFA.
- **Ruta B (Local):** En dependencias sin dominio, el Administrador Local deberá resetear la cuenta previa identificación visual del usuario y asentar el cambio en la **Bitácora de Eventos (F-AL-03)**.

4.3. Procedimiento de Baja e Inhabilitación (Ruta Crítica)

Este es el paso más importante para evitar "cuentas fantasma":

1. **Notificación Inmediata:** Recursos Humanos debe enviar un "Ticket de Baja" a IT en el momento en que se firma el acta de entrega-recepción física.
2. **Bloqueo en Cascada:**

- Paso 1: Deshabilitar cuenta de Active Directory (corta acceso a PC y red).
- Paso 2: Suspender buzón de correo institucional.
- Paso 3: Revocar acceso a sistemas específicos (Tesorería, Catastro, etc.).

3. **Preservación:** La cuenta no se borra de inmediato; se mantiene inhabilitada por 30 días para permitir la recuperación de información institucional si fuera necesario.

4.4. Control de Privilegios Elevados (Administradores)

1. **Cuentas Nominales:** Los técnicos no deben usar la cuenta "Administrator". Deben usar una cuenta personal con prefijo (ej. *adm-juanperez*).
2. **Bitácora de Superusuario:** Toda acción realizada con privilegios de administrador en servidores o bases de datos debe generar un log automático o quedar asentada en una bitácora técnica de cambios.
3. **Revisión Trimestral:** La Dirección de IT revisará que la lista de administradores no crezca injustificadamente.

4.5. Procedimiento para el Acceso Remoto (Teletrabajo)

Para los colaboradores que trabajan fuera de la oficina:

1. **Uso de VPN:** El acceso a la red interna solo se permite mediante túneles cifrados (VPN).
2. **Doble Candado:** Para conectar la VPN, es estrictamente obligatorio el **MFA mediante aplicación o token**, no se permite solo contraseña para accesos externos.
3. **Validación de Dispositivo:** El sistema de acceso lógico verificará que el equipo remoto tenga el antivirus institucional activo antes de permitir la conexión.

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

5. Definiciones

- **Active Directory (AD):** Servicio de directorio para redes de dominios Windows, utilizado por el 70% del Ayuntamiento para la gestión centralizada de identidades y permisos.
- **Autenticación Multi-Factor (MFA):** Método de control de seguridad que requiere al menos dos formas de identificación antes de conceder acceso (ej. algo que el usuario **sabe** como una contraseña, y algo que el usuario **tiene** como un código en su celular).

- **Control de Acceso Basado en Roles (RBAC):** Método de restringir el acceso a usuarios autorizados basándose en su función dentro de la organización, facilitando la administración masiva de permisos.
- **Cuentas Huérfanas:** Cuentas de usuario que permanecen activas después de que el titular ha dejado de colaborar con la organización; representan uno de los mayores riesgos de seguridad.
- **Identificador de Usuario (ID):** Cadena única de caracteres que permite al sistema reconocer a un individuo específico.
- **MFA (Autenticación Multi-Factor):** El "segundo candado" obligatorio que valida la identidad del usuario a través de un medio físico o digital adicional a la contraseña.
- **Principio de Menor Privilegio:** Concepto de seguridad que dicta que a un usuario se le deben otorgar solo los permisos mínimos necesarios para realizar su trabajo.

6. Formatos

Para mantener la "cancha" operativa, estos formatos pueden ser implementados en papel, archivos de Excel protegidos, o formularios dentro de una plataforma de tickets (tipo GLPI o Jira):

- **F-AL-01: Solicitud de Alta / Modificación de Accesos Lógicos**
  - *Propósito:* Documentar quién autoriza el acceso y qué permisos específicos (roles) se le asignan al nuevo colaborador.
- **F-AL-02: Inventario y Revisión de Cuentas de Usuario**
  - *Propósito:* Utilizado para la revisión semestral por parte de los titulares de área para confirmar que quienes tienen acceso aún laboran ahí y tienen el puesto correcto.
- **F-AL-03: Bitácora de Uso de Cuentas de Administrador y Terceros**
  - *Propósito:* Registro manual o automático de las sesiones iniciadas por personal técnico o proveedores externos para realizar tareas de mantenimiento.
- **F-AL-04: Lista de Verificación (Checklist) de Baja de Usuario**
  - *Propósito:* Asegurar que, al momento del despido o renuncia, se bloqueen todos los frentes: AD, Correo, Sistemas locales y VPN.

H. Ayuntamiento de Morelia

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

Esta tabla es tu respaldo ante cualquier auditoría, demostrando que el sistema es integral:

Control Anexo A	Nombre del Control	Descripción del Cumplimiento
5.15	**Control de acceso**	Se cumple mediante la política de permisos basados en roles (RBAC) y el principio de menor privilegio.
5.16	**Gestión de identidad**	Se garantiza a través de la identificación unívoca y el ciclo de vida del usuario (altas/bajas) descrito en el punto 4.
5.17	**Información de autenticación**	Se aborda con la política de complejidad de contraseñas y la prohibición de compartir credenciales.
5.18	**Derechos de acceso**	Se materializa en la revisión semestral de privilegios y el proceso de revocación inmediata ante bajas.
8.2	**Derechos de acceso privilegiado**	Se cumple con la restricción de cuentas de administrador y el uso de cuentas nominales para técnicos.
8.5	**Autenticación segura**	**Cumplimiento crítico:** Se garantiza mediante la declaración del **MFA como obligatorio** para todos los accesos.