Tabla de contenido

1. Propósito

El presente documento tiene como objetivo establecer los lineamientos y controles para asegurar que el acceso, procesamiento y almacenamiento de la información del H. Ayuntamiento de Morelia por parte de **proveedores externos y servicios en la nube** se realice bajo estándares estrictos de seguridad. Se busca mitigar los riesgos asociados a la cadena de suministro tecnológica y garantizar la continuidad de los servicios ciudadanos alojados en infraestructuras de terceros.

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

- **Estandarización de la Selección:** Garantizar que todo proveedor o servicio de nube sea evaluado técnicamente antes de su contratación, asegurando que sus controles de seguridad sean equivalentes o superiores a los del Ayuntamiento.
- **Formalización de Responsabilidades (Modelo de Responsabilidad Compartida):** Definir con claridad qué aspectos de seguridad corresponden al proveedor de nube (ej. Azure, AWS, Google Cloud) y cuáles son responsabilidad de la Dirección de TI del Ayuntamiento (ej. configuración, cifrado y gestión de identidades).
- **Protección Jurídica y Contractual:** Asegurar que todos los contratos incluyan cláusulas de confidencialidad (NDA), niveles de servicio (SLA) y el derecho a realizar auditorías de seguridad sobre los servicios prestados.
- **Control del Ciclo de Vida del Tercero:** Establecer un proceso ordenado para el alta, monitoreo y, especialmente, la baja de proveedores, garantizando la recuperación de activos y la eliminación segura de datos institucionales al finalizar la relación.
- **Gobernanza de Datos en la Nube:** Asegurar que la información de los ciudadanos de Morelia almacenada en la nube cumpla con las leyes de soberanía y protección de datos, evitando la fuga de información por configuraciones incorrectas o accesos no autorizados.
- **Resiliencia y Disponibilidad:** Evaluar la capacidad de recuperación ante desastres de los proveedores de nube para garantizar que, ante una falla técnica del tercero, los servicios críticos del Ayuntamiento (como recaudación o seguridad pública) no se vean interrumpidos.

Esta política es de **cumplimiento obligatorio** para todas las dependencias del H. Ayuntamiento de Morelia, así como para cualquier persona física o moral que preste servicios externos. El alcance se define en los siguientes tres niveles:

2.1. Alcance sobre Servicios en la Nube

Aplica a cualquier modalidad de servicio contratado que resida fuera de las instalaciones físicas del Ayuntamiento:

- **Infraestructura como Servicio (IaaS):** Servidores virtuales, almacenamiento y redes (ej. AWS EC2, Azure VMs).

- **Plataforma como Servicio (PaaS):** Bases de datos administradas y entornos de desarrollo (ej. Google App Engine, Azure SQL).
- **Software como Servicio (SaaS):** Aplicaciones listas para usar (ej. Microsoft 365, sistemas de nómina en la nube, herramientas de gestión de proyectos).
- **Nubes Híbridas y Privadas:** Cualquier combinación de infraestructura local con servicios externos.

2.2. Alcance sobre Proveedores y Terceros

Rige la relación con entidades externas que tengan acceso a información o infraestructura institucional:

- **Proveedores de TI:** Soporte técnico, mantenimiento de hardware, administración de redes y telecomunicaciones.
- **Fábricas de Software:** Empresas externas encargadas de desarrollar o mantener aplicaciones para el Ayuntamiento.
- **Servicios Profesionales:** Consultores, auditores externos y asesores que procesen datos sensibles.
- **Proveedores de Servicios Generales:** Empresas de vigilancia, limpieza o mantenimiento físico que tengan acceso a áreas restringidas como el SITE.

2.3. Alcance sobre el Ciclo de Vida del Dato y el Servicio

La política cubre todas las fases de la relación comercial y técnica:

- **Pre-contratación:** Evaluación de riesgos y debida diligencia de seguridad.
- **Operación:** Monitoreo de niveles de servicio (SLAs) y cumplimiento de controles de seguridad.
- **Terminación:** Procedimientos de salida, devolución de activos y borrado seguro de datos en la nube del tercero.

2.4. Exclusiones

Quedan excluidos de esta política los proveedores que no tengan acceso a información confidencial, datos personales de ciudadanos o infraestructura crítica (ej. proveedores de suministros de papelería que entregan solo en áreas de recepción).

3. Políticas de Seguridad para Proveedores y Servicios en la Nube

3.1. Selección y Debida Diligencia (Control 5.19)

Antes de cualquier contratación, la Dirección de TI debe realizar una evaluación de riesgos del proveedor:

- **Evaluación Técnica:** Todo proveedor de servicios críticos o de nube debe presentar sus certificaciones de seguridad (ej. ISO 27001, SOC2) o someterse a un cuestionario de seguridad institucional.
- **Criterios de Rechazo:** No se contratarán servicios de nube que no ofrezcan garantías de cifrado de datos, autenticación multifactor (MFA) y disponibilidad mínima según el SLA requerido por la dependencia.

3.2. Cláusulas de Seguridad en Contratos (Control 5.20)

Los contratos no son solo legales, son técnicos. Todo acuerdo con terceros debe incluir:

- **Derecho a Auditoría:** El Ayuntamiento se reserva el derecho de auditar (por sí mismo o por un tercero) los controles de seguridad del proveedor.
- **Confidencialidad (NDA):** Obligación de proteger la información del Ayuntamiento incluso después de terminada la relación laboral.
- **Notificación de Incidentes:** El proveedor está obligado a notificar cualquier brecha de seguridad que afecte los datos del Ayuntamiento en un plazo máximo de 24 horas.

3.3. Modelo de Responsabilidad Compartida y Responsabilidad Legal (Actualizado)

Se debe documentar con precisión el alcance de las obligaciones de cada parte:

- **Responsabilidad del Proveedor:** Seguridad física del centro de datos, infraestructura base (hipervisor) y redes troncales.
- **Responsabilidad del Ayuntamiento:** Configuración de firewalls en la nube, gestión de identidades (IAM), cifrado de datos y protección de aplicaciones.
- **Cláusula de Responsabilidad Civil y Penal:** En caso de una brecha de seguridad originada por negligencia o fallo en los controles del proveedor, el Ayuntamiento activará, además del Protocolo de Incidentes, las **acciones legales de rescisión**

contractual, ejecución de fianzas de cumplimiento y demandas por daños y perjuicios.

- **Cumplimiento de la LGPDPPSO:** El contrato debe estipular que el proveedor actúa como "Encargado" y que cualquier violación a la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* facultará al Ayuntamiento para colaborar con las autoridades (INAI/Instancia Estatal) en el fincamiento de sanciones directas al prestador del servicio.

3.4. Soberanía y Ubicación de los Datos

Dado que manejamos datos de ciudadanos de Morelia:

- **Residencia de Datos:** En la medida de lo posible, se preferirán proveedores que permitan elegir la región de almacenamiento de datos (ej. México o EE. UU.) para asegurar el cumplimiento con la Ley de Protección de Datos Personales.
- **Transferencias Internacionales:** Si el proveedor transfiere datos a otros países, debe garantizar que el nivel de protección sea equivalente al exigido por la normativa mexicana.

3.5. Gestión de Accesos para Terceros

- **Principio de Mínimo Privilegio:** Los proveedores solo tendrán acceso a los recursos estrictamente necesarios para cumplir su contrato.
- **Accesos Temporales:** Las cuentas para soporte técnico externo deben estar deshabilitadas por defecto y activarse solo durante la ventana de mantenimiento aprobada.
- **Autenticación Robusta:** Es obligatorio el uso de **MFA** para cualquier acceso de administración a consolas de nube o conexiones remotas de proveedores.

H. Ayuntamiento de Morelia

3.6. Monitoreo y Revisión del Servicio (Control 5.22)

- **Revisiones Periódicas:** Al menos una vez al año, se revisará el cumplimiento de los niveles de servicio (SLA) y los controles de seguridad de los proveedores críticos.
- **Gestión de Cambios del Tercero:** El proveedor debe informar sobre cambios significativos en su infraestructura o en la ubicación de sus centros de datos que puedan afectar el riesgo del Ayuntamiento.

3.7. Terminación de la Relación (Offboarding)

- **Recuperación de Activos:** Al finalizar el contrato, el proveedor debe devolver toda la información en un formato legible y útil para el Ayuntamiento.
- **Borrado Seguro:** El proveedor debe certificar la eliminación definitiva de cualquier copia o respaldo de los datos institucionales en su infraestructura o nube.

4. Procedimientos

4.1. Clasificación y Debida Diligencia Diferenciada

El proceso de selección varía según la naturaleza del proveedor:

1. **Proveedores Locales o a Medida:** Se les somete al llenado del **F-PRO-01 (Cuestionario de Evaluación)**. Deben demostrar solvencia técnica y permitir visitas de auditoría si se requiere.
2. **Proveedores Globales de Nube (Hyperscalers):** Debido a que no aceptan cuestionarios personalizados, el procedimiento consiste en la **descarga y validación de sus reportes de cumplimiento estándar** (ej. SOC 2 Type II, ISO 27001, PCI-DSS) desde sus portales de confianza (como AWS Artifact o Azure Trust Center).

4.2. Formalización Jurídica y Análisis de Adhesión

Dependiendo de la capacidad de negociación, se seguirá uno de estos dos caminos:

- **Vía Contractual (Proveedores Críticos):** Firma obligatoria de un contrato civil/mercantil que incluya el **NDA (Convenio de Confidencialidad)** y cláusulas de penalización por brechas de seguridad. No se iniciará ningún servicio sin estas firmas físicas o digitales.
- **Vía de Adhesión (Grandes Nubes):** Ante la imposibilidad de modificar los términos de Google o Amazon, la Dirección de TI debe ejecutar una **Revisión Exhaustiva de los SLA y Contratos de Adhesión**. Se utilizará el **F-PRO-03** para verificar que la disponibilidad ofrecida (ej. 99.9%) y las políticas de privacidad de la plataforma se alineen con la criticidad del sistema del Ayuntamiento.

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

4.3. Implementación y Modelo de Responsabilidad Compartida

Independientemente del tamaño del proveedor, se debe establecer la frontera de seguridad:

1. **Llenado de la Matriz (F-PRO-02):** Se definirá qué controles opera el proveedor (ej. seguridad física del datacenter) y cuáles opera el Ayuntamiento (ej. cifrado de la base de datos y gestión de usuarios).
2. **Configuración de Seguridad en Nube (Cloud Hardening):** * Se activará el **MFA (Multifactor Authentication)** para todas las cuentas con privilegios de administrador en la consola de la nube.
    - Se configurarán alertas de facturación y de seguridad para detectar anomalías en el consumo o accesos sospechosos desde ubicaciones no autorizadas.

4.4. Monitoreo de Niveles de Servicio (SLA) y Soporte

1. **Vigilancia de Disponibilidad:** Se utilizarán herramientas de monitoreo externas para validar que el proveedor cumpla con el tiempo de actividad prometido en el SLA.
2. **Accesos de Soporte:** Para proveedores locales, el acceso remoto será supervisado y temporal. Para grandes proveedores, se utilizarán las herramientas de "Lockbox" o aprobación de acceso que ofrece la plataforma nube, garantizando que el personal del proveedor solo entre a los datos si el Ayuntamiento lo autoriza explícitamente.
3. **Acciones Legales:** Si el monitoreo detecta una falla atribuible al proveedor, se procederá a:
    - Reclamar los créditos de servicio estipulados en el SLA.
    - Iniciar acciones legales por incumplimiento si la falla deriva en pérdida de datos o afectación grave a la ciudadanía.

H. Ayuntamiento de Morelia

4.5. Terminación y Garantía de Borrado Seguro

1. **Estrategia de Salida (Exit Strategy):** Para evitar el "Vendor Lock-in" (quedar atrapado con un proveedor), se realizarán pruebas semestrales de exportación de datos para asegurar que la información pueda ser migrada si la relación termina.
2. **Certificado de Borrado:** * **Proveedores Locales:** Deben entregar el **F-PRO-05** firmado, certificando la destrucción de copias.
    - **Proveedores Globales:** Se debe ejecutar el procedimiento de "Cierre de Cuenta y Purga de Datos" siguiendo la documentación oficial del proveedor, la cual garantiza la eliminación lógica y física de los recursos en sus granjas de servidores tras un periodo de gracia.

5. Definiciones

- **Contrato de Adhesión:** Términos y condiciones estandarizados impuestos por grandes proveedores de servicios (ej. AWS, Google, Azure) donde el Ayuntamiento no tiene capacidad de negociación. En estos casos, la seguridad se garantiza mediante la revisión de sus certificaciones (ISO 27001, SOC2) y sus niveles de servicio (SLA).
- **SLA (Service Level Agreement):** Acuerdo de Nivel de Servicio que define los tiempos de respuesta, disponibilidad (uptime) y penalizaciones en caso de fallos por parte del proveedor.
- **NDA (Non-Disclosure Agreement):** Convenio de Confidencialidad que obliga al proveedor a no revelar información sensible. Es obligatorio para proveedores locales o a medida.
- **Debida Diligencia (Due Diligence):** Proceso de investigación técnica y legal previo a la contratación para asegurar que el proveedor es confiable.
- **Modelo de Responsabilidad Compartida:** Marco que define qué parte de la seguridad es responsabilidad del proveedor de nube y cuál es responsabilidad del Ayuntamiento (ej. el proveedor asegura el servidor físico, el Ayuntamiento asegura la base de datos).

6. Formatos

Para que la gestión de terceros sea transparente y auditable, el Ayuntamiento utilizará los siguientes registros:

1. **F-PRO-01: Cuestionario de Evaluación y Análisis de Riesgos de Proveedores.**
2. **F-PRO-02: Matriz de Responsabilidad Compartida (Ayuntamiento vs. Proveedor).**
3. **F-PRO-03: Lista de Verificación para Revisión de Contratos de Adhesión y SLAs.**
    - *Nota:* Este formato es específico para grandes proveedores, donde se valida que el SLA cumpla con los requisitos de disponibilidad del Ayuntamiento.
4. **F-PRO-04: Registro de Firmas de NDA y Convenios de Confidencialidad.**
5. **F-PRO-05: Acta de Terminación de Servicio y Certificado de Borrado Seguro.**

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

7. Relación Normativa (ISO 27001:2022)

Este documento asegura el cumplimiento de los controles de la cadena de suministro y servicios externos:

Control	Título	Justificación del Cumplimiento
5.19	**Seguridad en la relación con proveedores**	Establece el marco para evaluar a terceros antes de la contratación.
5.20	**Abordar la seguridad en acuerdos**	Garantiza la revisión de cláusulas en contratos locales y de adhesión en nube.
5.23	**Seguridad en servicios de nube**	Define la gobernanza técnica de las plataformas externas (Azure, AWS, Google).
5.22	**Monitoreo y revisión de servicios**	Asegura que se auditen los SLAs y el desempeño de los proveedores críticos anualmente.

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