Tabla de contenido

1. Propósito

El propósito de este documento es establecer las directrices de seguridad de la información que deben regir durante todo el ciclo de vida de los colaboradores en el **H. Ayuntamiento de Morelia** (desde el reclutamiento hasta la desincorporación).

Se busca profesionalizar la gestión del capital humano bajo un enfoque de seguridad, garantizando que:

- **Protección desde el origen:** Se asegure la privacidad de los candidatos desde el primer contacto, cumpliendo con las leyes de protección de datos personales.
- **Idoneidad y Confianza:** Se implementen mecanismos de verificación para asegurar que el personal contratado cuente con la integridad y competencias necesarias para el manejo de información institucional.
- **Compromiso Legal:** Se formalice la responsabilidad del colaborador mediante acuerdos de confidencialidad que trasciendan la duración de su contrato.
- **Sincronización Operativa:** Se establezca un flujo de comunicación ininterrumpido entre las áreas administrativas y la Dirección de TI para que la asignación y revocación de activos (físicos y lógicos) sea precisa y oportuna.
- **Gestión del Riesgo en la Separación:** Se minimicen los riesgos de fuga de información o sabotaje durante los procesos de baja, especialmente en situaciones de conflicto o bajas no conciliadas.

2. Alcance

Esta política es de cumplimiento obligatorio para todas las dependencias del H. Ayuntamiento de Morelia y aplica a todas las personas físicas que presten sus servicios en la institución, sin importar su nivel jerárquico o modalidad de contratación:

2.1. Clasificación de Sujetos

- **Candidatos:** Personas en proceso de selección o reclutamiento.
- **Personal de Estructura:** Empleados de base y de confianza.
- **Personal Temporal:** Contratos por tiempo determinado, honorarios, pasantes y prestadores de servicio social.
- **Terceros Vinculados:** Personal externo que, por la naturaleza de su servicio, esté asimilado a la operación diaria de una dependencia.

2.2. Fases del Ciclo de Vida cubiertas

- **Pre-empleo:** Selección, reclutamiento y debida diligencia.
- **Durante el empleo:** On-boarding, cambios de puesto, promociones, sensibilización y capacitación en seguridad.
- **Cese o Cambio de Empleo:** Off-boarding (bajas conciliadas y no conciliadas), revocación de accesos y recuperación de activos.

2.3. Flexibilidad Administrativa

Dado que la estructura de gestión de personal puede variar entre dependencias, las responsabilidades aquí descritas recaerán en:

1. La **Dirección de Administración** (en procesos centralizados).
2. La **Coordinación Administrativa** o el **Enlace de Capital Humano** de cada dependencia (en procesos descentralizados).
3. El **Titular de la Dependencia** en ausencia de las figuras anteriores.

3. Políticas de Gestión del Capital Humano

3.1. Reclutamiento y Selección Segura

- **Transparencia y Privacidad Inicial:** Desde la primera interacción con cualquier candidato (recepción de CV, entrevista inicial o llenado de solicitud), el responsable del proceso debe poner a su disposición el **Aviso de Privacidad Integral** del Ayuntamiento. Este paso es obligatorio para dar cumplimiento a la Ley de Protección de Datos Personales.
- **Debida Diligencia (Screening):** Antes de la contratación, se deben realizar verificaciones proporcionales al nivel de acceso a la información que tendrá el puesto. Esto incluye validación de antecedentes académicos, profesionales y, en puestos críticos (como Tesorería o TI), una revisión más exhaustiva conforme a la normativa legal vigente.

3.2. Formalización y Compromiso de Confidencialidad

- **Acuerdos de Confidencialidad (NDA):** Todo colaborador, sin excepción, debe firmar un **Acuerdo de Confidencialidad y No Divulgación** como anexo a su contrato o nombramiento.
- **Vigencia Post-Empleo:** Los acuerdos de confidencialidad deben estipular explícitamente que la obligación de resguardo de la información institucional permanece vigente incluso después de terminada la relación laboral, por el tiempo que las leyes aplicables (en materia de responsabilidades administrativas y protección de datos) determinen.
- **Aceptación de Políticas:** Durante la firma, el colaborador debe manifestar por escrito que conoce y se compromete a cumplir con el Manual de Seguridad de la Información del Ayuntamiento.

3.3. Proceso de On-boarding (Alta y Asignación)

- **Notificación Obligatoria a TI:** El responsable administrativo de la dependencia debe notificar al área de TI sobre el ingreso de un nuevo colaborador con una anticipación mínima de 48 horas.
- **Sincronización de Activos:** La asignación de herramientas de trabajo está condicionada a esta notificación. El proceso incluye:
  - Creación de identidad digital (Usuario y Correo Institucional).
  - Entrega de equipo de cómputo y periféricos bajo firma de **Resguardo de Activos**.
  - Alta en los sistemas de control de acceso físico (biométricos o entrega de llaves).
- **Integración al Active Directory**. Todos los equipos deben estar integrados al Active Directory del Ayuntamiento de Morelia, gestionado por la Agencia de la Ciudad Inteligente y Transformación digital a través del área de TI o responsable administrativo en cada Dependencia o Entidad, desde el momento de la compra o asignación.

3.4. Cambios de Puesto y Movilidad Interna

- **Actualización de Perfiles:** Cuando un colaborador sea promovido o transferido, el responsable administrativo debe notificar el cambio para ejecutar una "limpieza de privilegios".
- **Recolección y Reasignación:** Se deben recuperar los activos o llaves del puesto anterior antes de otorgar los nuevos, evitando la acumulación de accesos innecesarios (derechos de acceso residuales).

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

3.5. Proceso de Off-boarding (Bajas y Terminación)

- **Revocación Inmediata de Accesos:** Ante la baja de un colaborador, la notificación a TI debe ser prioritaria. La inhabilitación de cuentas lógicas debe ocurrir, idealmente, de forma simultánea a la firma de la baja administrativa.
- **Protocolo para Bajas No Conciliadas:** En casos de despido conflictivo, rescisión o bajas no conciliadas, el responsable administrativo debe coordinar con TI un **bloqueo preventivo de accesos** minutos antes de notificar al colaborador sobre su situación, para evitar cualquier intento de sabotaje, borrado o extracción de información.
- **Recuperación de Activos:** No se podrá finalizar el proceso administrativo de baja (como el pago de finiquito o última nómina) sin la previa entrega de la **Hoja de**

Liberación de Activos, firmada por el área de TI y el responsable de Patrimonio, garantizando que se devolvieron equipos, llaves, tokens y credenciales.

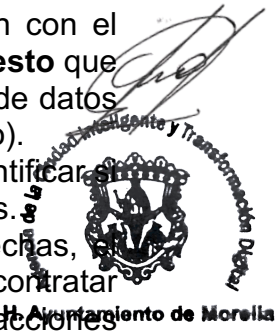
3.6. Sensibilización y Capacitación

- **Programa de Concientización:** Todo nuevo ingreso debe recibir una inducción básica en seguridad de la información.
- **Recordatorios Periódicos:** Independientemente de la dependencia, todos los colaboradores deben participar en al menos una sesión anual de actualización sobre riesgos digitales, phishing y manejo seguro de documentos físicos.

3.7. Competencia en Seguridad de la Información

La institución debe asegurar que el personal que realiza trabajos que afectan el desempeño de la seguridad de la información sea competente.

- **Determinación de la Competencia:** Cada dependencia, en coordinación con el área administrativa y la Dirección de TI, deberá definir un **Perfil de Puesto** que incluya las competencias necesarias en materia de seguridad (ej. manejo de datos personales para administrativos o seguridad de redes para personal técnico).
- **Evaluación de Brechas:** Anualmente se realizará una evaluación para identificar si el colaborador cuenta con la educación, formación o experiencia adecuadas.
- **Acciones de Adquisición de Competencia:** En caso de detectarse brechas, el Ayuntamiento se compromete a proporcionar la formación necesaria, contratar expertos o reasignar funciones, evaluando siempre la **eficacia** de las acciones tomadas.



3.8. Conciencia y Sensibilización

No basta con que el personal sea capaz; debe estar "consciente". Todo el capital humano bajo el alcance del SGSI debe tener claridad sobre:

- **La Política de Seguridad:** Conocer su existencia, dónde consultarla y cómo se alinea con los objetivos del Ayuntamiento.
- **Su contribución personal:** Entender que un escritorio limpio o una contraseña robusta son piezas clave para la eficacia del sistema.
- **Implicaciones del Incumplimiento:** Conocer las consecuencias legales, administrativas y de seguridad que conlleva no seguir los lineamientos establecidos.

3.9. Programa Anual de Capacitación y Formación

Se establecerá un calendario de formación continua dividido en tres niveles de profundidad:

1. **Nivel General (Inducción):** Obligatorio para todo nuevo ingreso. Temas: Aviso de privacidad, uso de activos y reporte de incidentes.
2. **Nivel Operativo (Específico):** Para personal que maneja datos sensibles o trámites ciudadanos. Temas: Clasificación de información y protección de PII (Personal Identifiable Information).
3. **Nivel Técnico (Especializado):** Para personal de la Dirección de TI y enlaces técnicos. Temas: Hardening, gestión de vulnerabilidades y respuesta a incidentes.

3.10. Evidencia y Registros de Capital Humano

Para que el SGSI sea auditable, la gestión del capital humano debe generar y custodiar evidencia documental de:

- Curriculums y certificados que avalen la competencia inicial.
- Listas de asistencia y evaluaciones de los cursos de capacitación.
- Acuerdos de confidencialidad (NDA) debidamente firmados.
- Constancias de recepción de las políticas institucionales.

4. Procedimientos

4.1. Procedimiento de Reclutamiento y Selección Segura

Este procedimiento inicia desde que surge la necesidad de la vacante y termina con la decisión de contratación.

- **Privacidad:** Antes de recibir cualquier documento, el Responsable Administrativo debe entregar el **Aviso de Privacidad Integral**. El candidato debe firmar el acuse de recibo. Sin esta firma, no se procesa ninguna información.
- **Recepción de Candidatura:** Se recibe el CV y se verifica que los datos sensibles (como domicilio o teléfono) sean tratados conforme al aviso de privacidad.
- **Validación de Competencia Inicial:** Se coteja el perfil del candidato contra la **Matriz de Competencias** del puesto. Se deben verificar físicamente los títulos, cédulas y certificaciones que avalen el conocimiento técnico en el área.

- **Debida Diligencia:** El Responsable Administrativo contactará a los últimos dos empleadores para validar referencias. En puestos que manejan información financiera o técnica crítica, se realizará una entrevista de integridad.

4.2. Procedimiento de On-boarding (Alta y Activación)

Este procedimiento asegura que el colaborador tenga lo necesario para trabajar, bajo un marco de seguridad total.

- **Disparador de IT:** Una vez confirmada la contratación, el Responsable Administrativo envía a la Dirección de TI el formato **F-CH-01 (Alta de Usuario)**.
  - *Nota:* Este envío debe ocurrir con **48 horas de anticipación** al ingreso.
- **Preparación de Activos:** El área de TI asigna el equipo (previo hardening), crea la cuenta de Active Directory, correo institucional y configura los permisos de acceso a sistemas según el perfil de puesto, previa firma de Cartas Responsivas para cada Sistema o conexión.
- **Día de Ingreso - Firma Legal:** El colaborador firma, antes de recibir cualquier activo:

  1. Contrato o Nombramiento.
  2. **Acuerdo de Confidencialidad y No Divulgación (NDA)** (Vigencia según Ley de Responsabilidades Administrativas).
  3. Carta de Aceptación de la Política de Seguridad de la Información.

- **Entrega de Activos:** Se entregan los equipos y cuentas bajo el formato de **Resguardo de Activos**. Se entrega la clave temporal de acceso, la cual el sistema obligará a cambiar en el primer inicio de sesión.
- **Inducción:** El colaborador debe completar en su primera semana el curso básico de "Conciencia en Seguridad de la Información".

4.3. Procedimiento de Gestión de Competencia y Conciencia

Para garantizar que el personal sea apto y consciente de los riesgos.

- **Definición de Necesidades:** Cada enero, los titulares de área identifican las brechas de competencia (ej. necesidad de curso sobre Ley de Protección de Datos).
- **Ejecución del Plan:** Se imparten sesiones de formación. Cada sesión debe generar una **Lista de Asistencia** y una **Evaluación de Conocimiento**.

- **Medición de Eficacia:** Tres meses después del curso, el Responsable Administrativo enviará una encuesta o prueba práctica para verificar si la competencia se aplicó en el trabajo diario.
- **Campañas de Conciencia:** Mensualmente, el área técnica enviará "Cápsulas de Seguridad" vía correo electrónico sobre temas de actualidad (phishing, escritorio limpio, etc.).

4.4. Procedimiento de Off-boarding Conciliado (Baja Administrativa)

Para salidas planeadas (renuncias, fin de contrato).

- **Notificación:** El Responsable Administrativo notifica a TI la fecha exacta del último día laboral del colaborador.
- **Inventario de Devolución:** Se utiliza el **Checklist de Devolución (F-CH-02)** para recuperar físicamente: Laptops, celulares, llaves, tokens y credenciales de acceso.
- **Inhabilitación Programada:** A las 18:00 hrs del último día, TI deshabilita la cuenta de Active Directory y el correo electrónico.
- **Cierre de Expediente:** Se anexa la hoja de liberación de activos al expediente del colaborador para permitir el trámite del finiquito.

4.5. Procedimiento de Off-boarding No Conciliado (La "Ruta Crítica")

Para bajas conflictivas, rescisiones o despidos inmediatos. **Este procedimiento es de máxima prioridad.**

- **Sincronización Silenciosa:** El Responsable Administrativo se comunica vía telefónica o canal privado con el Director de TI para coordinar el momento exacto del despido.
- **Bloqueo Preventivo: 15 minutos antes** de que el colaborador sea llamado a la oficina para la notificación, TI ejecutará:
    1. Corte de sesión activa de VPN.
    2. Cambio de contraseña y deshabilitación de cuenta de Active Directory.
    3. Bloqueo de correo electrónico en dispositivos móviles.
- **Notificación y Recuperación:** Mientras se le notifica la baja, un enlace administrativo acude a la estación de trabajo del colaborador para resguardar físicamente el equipo de cómputo.
- **Acompañamiento:** El colaborador solo podrá retirar objetos personales de su escritorio bajo supervisión, sin permiso de manipular ningún teclado o dispositivo de almacenamiento.

- **Revocación Física:** Se recuperan inmediatamente las llaves de oficinas y tarjetas de acceso.

5. Definiciones

- **Acuerdo de Confidencialidad (NDA):** Contrato legal que vincula al colaborador a mantener en secreto la información sensible a la que tenga acceso, con validez incluso después de terminada la relación laboral.
- **Aviso de Privacidad:** Documento físico o digital que informa al candidato o colaborador sobre qué datos personales se recaban, para qué fin y cómo se protegen, conforme a la Ley de Protección de Datos Personales.
- **Baja No Conciliada:** Término de la relación laboral bajo condiciones de conflicto, rescisión o despido, que requiere protocolos de seguridad física y lógica inmediatos para prevenir sabotajes.
- **Capital Humano:** El conjunto de conocimientos, habilidades y aptitudes de los colaboradores que agregan valor a la institución y que deben ser gestionados bajo criterios de riesgo.
- **Competencia:** Capacidad demostrada para aplicar conocimientos y habilidades con el fin de alcanzar los resultados previstos en seguridad de la información.
- **Conciencia (Awareness):** El estado de entendimiento de los colaboradores sobre la importancia de la seguridad de la información y su responsabilidad personal en el éxito del sistema.
- **Debida Diligencia (Screening):** Proceso de verificación de antecedentes y referencias para asegurar la idoneidad de un candidato antes de su contratación.

6. Formatos

Para que esta "receta" sea ejecutable, se establecen los siguientes formatos base que deben ser custodiados por el responsable administrativo de cada dependencia:

- **F-CH-01: Registro de Alta de Colaborador y Solicitud de Activos**
  - *Uso:* Disparador para que IT cree cuentas y prepare el equipo endurecido.
- **F-CH-02: Checklist de Devolución de Activos (Off-boarding)**
  - *Uso:* Inventario físico de entrega (laptops, llaves, tokens) previo a la baja definitiva.
- **F-CH-03: Acuerdo de Confidencialidad y No Divulgación (NDA)**
  - *Uso:* Documento legal anexo al contrato/nombramiento.
- **F-CH-04: Matriz de Competencias y Seguimiento de Capacitación**

- *Uso:* Control de qué cursos ha tomado cada colaborador y su evaluación de eficacia.

- **F-CH-05: Acuse de Recibo de Aviso de Privacidad y Políticas de Seguridad**
  - *Uso:* Evidencia de cumplimiento legal desde el primer contacto con el candidato.

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

Este documento es el soporte documental principal para las siguientes cláusulas y controles:

Cláusula / Control	Título	Descripción del Cumplimiento
Cláusula 7.2	**Competencia**	Se cumple mediante la Matriz de Competencias y los procedimientos de evaluación de eficacia (Punto 4.3).
Cláusula 7.3	**Concientización**	Se materializa con el Programa Anual de Capacitación y las campañas mensuales de sensibilización.
Control A.6.1	**Investigación de antecedentes**	Implementado en el proceso de Reclutamiento y Selección Segura (Debida diligencia).
Control A.6.2	**Términos y condiciones de empleo**	Cubierto por la firma obligatoria del NDA y la aceptación de políticas en el On-boarding.
Control A.6.4	**Acciones disciplinarias**	Referenciado en las implicaciones por incumplimiento dentro de las políticas de conciencia.
Control A.6.5	**Responsabilidades al término**	Se garantiza con el proceso de Off-boarding y la vigencia post-empleo del NDA.
Control A.6.6	**Confidencialidad o acuerdos de no divulgación**	Asegurado mediante el formato F-CH-03 obligatorio para todo el personal.