POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN TRATAMIENTO DEL INSTITUTO MUNICIPAL DE LAS MUJERES DE LEÓN, GUANAJUATO.

DRA. IVONNE JANNETTE PÉREZ WILSON, EN MI CARÁCTER DE DIRECTORA GENERAL DEL INSTITUTO MUNICIPAL DE LAS MUJERES DE LEÓN, GUANAJUATO, CON FUNDAMENTO EN LO ESTABLECIDO EN EL ARTÍCULO 34 FRACCIONES I, IV, XXIX DEL REGLAMENTO DEL INSTITUTO MUNICIPAL DE LAS MUJERES DE LEÓN, GUANAJUATO, ME PERMITO EMITIR LAS SIGUIENTES:

POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN TRATAMIENTO DEL INSTITUTO MUNICIPAL DE LAS MUJERES DE LEÓN, GUANAJUATO.

INTRODUCCIÓN

El Instituto Municipal de las Mujeres de León Guanajuato, es sujeto obligado, constituyéndose así, como entidad garante en materia de Protección de Datos Personales conforme a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Guanajuato.

Es responsable de proteger los datos personales que trate, garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad los deberes de seguridad y confidencialidad, así como las obligaciones derivadas de la Ley Estatal y General.

El presente documento constituye las Políticas Internas del Instituto Municipal de las Mujeres de León, Guanajuato, elaboradas en observancia al principio de responsabilidad, el cual prevé que el sujeto obligado responsable del tratamiento de los datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato, así como el Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Municipio de León, Guanajuato; y las Políticas Generales para la Protección de los Datos Personales en la Administración Pública Municipal de León, Guanajuato.

Siguiendo también a la información contenida en el Documento de Seguridad del Municipio de León, Guanajuato y los resultados obtenidos es que se realizan las presentes:

POLÍTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN TRATAMIENTO DEL INSTITUTO MUNICIPAL DE LAS MUJERES DEL MUNICIPIO DE LEÓN, GUANAJUATO.

CAPÍTULO PRIMERO

DISPOSICIONES GENERALES

Artículo 1.- Las presentes Políticas tienen por objeto desarrollar las disposiciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato.

Artículo 2.- Para efectos de la aplicación de estas Políticas, se entenderá por:

I. **Aviso de privacidad:** Documento que se pone a disposición de la persona titular de los datos personales, en cualquier formato que genere el responsable a partir del momento en el que recaben sus datos personales, con el objetivo de informarle los propósitos del tratamiento de los mismos;

II. **Bases de datos**: conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación tipo de soporte, procesamiento, almacenamiento y organización;

III. **Consentimiento:** manifestación de la voluntad libre, específica e informada de la persona titular, mediante la cual autoriza el tratamiento de sus datos personales;

IV. **Datos personales:** información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

V. **Datos personales sensibles:** aquella información que hace referencia a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a este. Se considera sensibles, de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual;

VI. **Derechos ARCOP:** Derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales;

VII. **IMMujeres:** Instituto Municipal de las Mujeres del Municipio de León, Guanajuato;

VIII. **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato;

IX. **Ley de Transparencia:** Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato;

X. **Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

XI. **Ley General de Transparencia:** Ley General de Transparencia y Acceso a la Información Pública;

XII. **Medidas de seguridad:** conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales;

XIII. **Medidas de seguridad físicas:** conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deberán considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización del responsable, sus instalaciones físicas, áreas críticas, recursos y datos personales;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pudiera salir de la organización del responsable, y
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

XIV. **Medidas de seguridad técnicas:** las acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deberá considerar las siguientes actividades:
a) Prevenir el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que la persona usuaria lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad de la adquisición, operación, desarrollo y mantenimiento de software y hardware, y
d) Gestionar las comunicaciones, operación y medios de almacenamiento de los recursos informáticos en el tratamiento de los datos personales;

XV. **Persona enlace:** Persona servidora pública de área designada para actuar de manera conjunta con la persona titular de la jefatura de transparencia en la protección de los datos personales en posesión del Instituto Municipal de las Mujeres de León, Guanajuato.

XVI. **Políticas generales:** Políticas generales para la protección de los Datos Personales en la Administración Pública Municipal de León Guanajuato;

XVII. **Reglamento de Transparencia:** Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Municipio de León, Guanajuato;

XVIII. **Responsable:** Sujeto obligado a que se refiere la fracción II del artículo 2 de la Ley que decide sobre el tratamiento de datos personales;

XIX. **Titular:** la persona física a quien corresponden los datos personales;

XX. **Tratamiento:** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales, y

XXI. **Unidad de Transparencia:** instancia a que se refiere el artículo 7 de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato.

Artículo 3.- Las presentes Políticas son de observancia general para todo el personal del Instituto Municipal de las Mujeres de León, Guanajuato, que se encuentre involucrado en el tratamiento de datos personales.

Artículo 4.- Las personas titulares de la Coordinación Jurídica, así como la Jefatura de Transparencia asesorarán de ser necesario al personal de las diferentes áreas del **IMMujeres** en materia de protección de datos personales conforme a los principios, deberes y obligaciones establecidos en la Ley General, las presentes Políticas y demás normativa aplicable.

Artículo 5.- Para las actividades señaladas en las presentes Políticas, se contará con personas servidoras públicas que actúen como enlaces en materia de datos personales.

Las personas titulares de las direcciones de área nombrarán por lo menos una persona servidora pública como enlace en materia de protección de datos personales, que actuará de manera conjunta con la persona titular de la jefatura de transparencia para la protección de los mismos y quienes en conjunto, verificarán la correcta implementación de las medidas de seguridad físicas, técnicas y administrativas previstas en las presentes Políticas.

Artículo 6.- Las personas titulares de las direcciones y coordinaciones de área, así como la persona enlace, son las responsables del tratamiento de los datos personales en el ámbito de sus facultades y atribuciones; y; por lo tanto, tendrán la obligación de cumplir los principios, deberes y obligaciones establecidos en la Ley General, las presentes Políticas y demás normatividad aplicable.

Artículo 7.- Lo no especificado en estas Políticas se regirá supletoriamente por la Ley, la Ley de Transparencia, la Ley General, la Ley General de Transparencia, Políticas generales, Reglamento de Transparencia y demás normativa aplicable.

CAPÍTULO SEGUNDO
DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Artículo 8.- Los principios de protección de datos personales, son las herramientas utilizadas para garantizar la efectiva protección de los datos personales de sus titulares cuando son tratados; herramientas que son de uso obligatorio para interpretar y aplicar la Ley General y demás normativa aplicable, además de representar un límite al tratamiento de datos personales que se encuentran en posesión de sujetos obligados, siendo los siguientes:

- **Principio de Licitud**: Se deberá tratar los datos con apego y cumplimiento a la normatividad vigente que resulte aplicable.

- **Principio de Finalidad**: El tratamiento de los datos debe estar justificado por las finalidades concretas, explícitas, lícitas y legítimas, relacionadas con las atribuciones expresas que la normatividad aplicable confiera.
- **Principio de Lealtad:** abstenerse de obtener y tratar los datos personales a través de medios engañosos o fraudulentos, privilegiando, en todo momento, la protección de los intereses del titular y su expectativa razonable de privacidad.

- **Principio de Consentimiento:** La persona responsable deberá obtener el consentimiento de la persona titular para el tratamiento de los datos personales, salvo que se actualice alguna excepción de las contempladas en la Ley.

- **Principio de Calidad:** Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales.

- **Principio de proporcionalidad:** La persona responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para las finalidades que justifican su tratamiento.
- **Principio de información:** La persona responsable deberá informar a la persona titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que puedan tomar decisiones informadas al respecto.

- **Principio de responsabilidad:** La persona responsable deberá implementar los mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones, así como para rendir cuentas a la persona titular y al instituto sobre los tratamientos de datos personales que efectúen, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales o de cualquier otro mecanismo que determine adecuado para tales fines.

CAPÍTULO TERCERO
DE LOS DEBERES PARA LA PROTECCIÓN DE DATOS PERSONALES

Artículo 9.- La protección de los datos personales, prevé dos deberes, el de confidencialidad y el de seguridad.

Artículo 10.- La importancia de estos deberes, es proteger los datos personales de cualquier amenaza de riesgo con potencial para provocarles un daño o perjuicio, como el robo, extravío o copia no autorizada, pérdida o destrucción no autorizada, uso o acceso no autorizado, daño, alteración o modificación no autorizada. Con los deberes se garantiza la confidencialidad, integridad y disponibilidad de los datos personales.

Artículo 11.- Las personas responsables del tratamiento de datos personales, con independencia del tipo de soporte en el que se encuentren o el tipo de tratamiento que se realice, deberán establecer las medidas de seguridad de carácter administrativo, físico y técnico que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso acceso o tratamiento no autorizado, y así garantizar su confidencialidad, integridad y disponibilidad.

Artículo 12.- Deber de confidencialidad: Las personas titulares de las Direcciones de área deberán establecer controles o mecanismos de observancia obligatoria para las personas servidoras públicas que intervengan en cualquier fase del tratamiento, con la finalidad de que mantengan en secreto la

información, evitando que los datos personales sean revelados a personas no autorizadas y previniendo la divulgación no autorizada de los mismos, obligación que subsistirá aún después de finalizar su relación laboral con IMMujeres.

Artículo 13.- Deber de seguridad: Cada persona de las diferentes áreas adscritas al IMMujeres, deberá adoptar las medidas físicas, técnicas y administrativas a través de las cuales garanticen la protección de datos personales que se detallan en el siguiente capítulo.

CAPÍTULO CUARTO
MEDIDAS DE SEGURIDAD FÍSICAS Y TÉCNICAS

Artículo 14.- Las personas titulares de las diferentes áreas del IMMujeres responsables del tratamiento de datos personales, verificarán que aquellos documentos que contengan datos personales sean restringidos únicamente para el uso y manejo del personal autorizado.

Artículo 15.- Los documentos físicos con datos personales se almacenarán en archivadores, cajones o espacios destinados que puedan ser cerrados con llave.

Artículo 16.- Para la consulta de expedientes físicos se deberá realizar el llenado de la bitácora correspondiente que obra en el espacio destinado para el archivo general.

Artículo 17.- A fin de evitar la reproducción o divulgación no autorizada de información, el personal adscrito al IMMujeres, deberá abstenerse de dejar documentos con datos personales o información confidencial en equipos como copiadoras, escáneres u otros mecanismos de impresión.

Artículo 18.- La documentación que contenga datos personales o información confidencial, ya sea considerada de comprobación administrativa inmediata o de archivo, deberá manejarse para su disposición final conforme a la normativa archivística aplicable.

Artículo 19.- Es necesario proteger los correos electrónicos, equipos de cómputo, sistemas y otros recursos con contraseñas seguras. Para evitar el acceso no autorizado a datos personales o información confidencial, se recomienda actualizar las contraseñas trimestralmente. Además, las contraseñas deben tener al menos 8 caracteres e incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.

Artículo 20.- El personal de las diferentes áreas del IMMujeres que posean información que contenga datos personales y datos personales sensibles en medios digitales, deberán solicitar a la persona titular de área de Tecnologías de la Información del IMMujeres la realización de respaldos periódicos y deberán ser resguardados de manera segura.

Artículo 21.- Reportar de manera inmediata a la persona titular del área de tecnologías de la información, a la persona titular de la jefatura de transparencia y a la persona enlace respecto a cualquier falla en sistemas, plataformas, programas o tecnologías que puedan comprometer datos personales o información confidencial, para que se tomen las medidas de protección necesarias.

Artículo 22.- Está prohibido para el personal de IMMujeres, copiar o transferir bases de datos institucionales a dispositivos externos sin autorización por escrito del jefe inmediato.

Artículo 23.- En caso de remitir de manera electrónica información a terceras personas que contengan datos personales se deberá realizar el cifrado de la misma.

Artículo 24.- En caso de remitir documentación de manera física a terceras personas, se deberá remitir la misma cuando aplique en sobre cerrado y ser remitidos únicamente con los técnicos estafetas asignados por el IMMujeres.

Artículo 25.- El personal adscrito al IMMujeres deberá implementar la política de escritorio limpio, que se hace referencia en el anexo 1.

Artículo 26.- Para dar cumplimiento a estas medidas, el personal de las diferentes áreas que realicen el tratamiento de datos personales deberá realizar de manera semestral la actualización de los inventarios de datos personales correspondientes.

Artículo 27.- En caso de atender una solicitud de acceso a la información que contenga datos personales y/o información sensible, se procederá a elaborar la versión pública o, en su defecto, a la reserva de dicha información.

Artículo 28.- En caso de que personal adscrito del IMMujeres requiera trasladar el equipo de cómputo asignado fuera de alguna de las instalaciones deberán contar con el pase de salida denominado “Préstamo de equipo de cómputo”, misma que se adjunta a la presente como **anexo 2**.

CAPÍTULO QUINTO
DOCUMENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES

Artículo 29.- Para la protección de Datos Personales, el IMMujeres, deberá contar con los siguientes documentos:

Aviso de privacidad: Documento generado para dar a conocer a las y los titulares los datos personales que son recabados y las finalidades de su tratamiento.

El IMMujeres deberá contar con un aviso de privacidad integral y su correlativo aviso de privacidad simplificado, por cada tratamiento de datos personales y si fuera el caso el consentimiento expreso.

Artículo 30.- Cuando se requiera la actualización o un nuevo aviso de privacidad en sustitución de los avisos de privacidad ya existentes, las personas titulares de las direcciones y coordinaciones de área, deberán solicitar vía correo electrónico a la persona titular de la jefatura de transparencia cuando se encuentre alguno de los siguientes supuestos:

- Por disposición Normativa;
- Cuando se requiera recabar datos personales adicionales a aquellos informados en el aviso de privacidad original, que no se obtengan de manera directa de la persona titular y se requiera de su consentimiento para el tratamiento de estos;

- Cuando cambien las finalidades señaladas en el aviso de privacidad original;
- En caso de que se modifiquen las condiciones de la transferencia de datos personales o se pretendan realizar otras no previstas inicialmente siendo necesario el consentimiento de la persona titular.

CAPÍTULO SEXTO
EJERCICIO DE LOS DERECHOS ARCOP

Artículo 31.- Se entenderá por ACCESO cuando la persona titular tiene derecho de consultar sus datos personales que obren en posesión del responsable, así como a conocer la información relacionada con las condiciones, generalidades y particularidades de su tratamiento.

Artículo 32.- La persona titular tendrá derecho de solicitar la RECTIFICACIÓN o CORRECCIÓN de datos personales, cuando estos resulten inexactos, incompletos o desactualizados.

Artículo 33.- Se origina la CANCELACIÓN cuando la persona titular tiene el derecho de solicitar la eliminación de sus datos personales de cualquier archivo, registro, expediente o sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados.

Artículo 34.- La OPOSICIÓN consiste en que la persona titular puede solicitar se cese el tratamiento de los mismos, cuando:

I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular; y

II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

En aquellos tratamientos de datos personales a que se refiere la fracción II del presente artículo, el responsable deberá informar al titular sobre la existencia del mismo e incluir una evaluación o valoración humana que, entre otras cuestiones, contemple la explicación de la decisión adoptada por la intervención humana.

En caso de resultar procedente el derecho de oposición, el responsable deberá cesar el tratamiento de los datos personales respecto de aquellas finalidades que resulten aplicables.

Artículo 35.- La PORTABILIDAD DE DATOS PERSONALES ocurre cuando los datos personales sean tratados por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos personales objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado, el cual le permita seguir utilizándolo.

Artículo 36.- La persona titular de la Coordinación Jurídica a través de la persona titular de la Jefatura de Transparencia turnará las solicitudes de ejercicio de derechos ARCOP que sean turnadas a IMMujeres a las áreas adscritas que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales, para que se pronuncien y den atención en los plazos y términos establecidos en la Ley.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transferir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable de quien se retiren los datos personales.

Para el ejercicio de este derecho, el responsable deberá considerar los lineamientos del Sistema Nacional relativos a los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

CAPÍTULO SÉPTIMO
TRANSFERENCIAS DE LOS DATOS PERSONALES

Artículo 37.- La transferencia de datos personales, es toda comunicación de datos personales, se nacional o internacional, se encuentra sujeta al consentimiento expreso de la persona titular salvo las excepciones previstas en la Ley, y la misma deberá ser informada al titular mediante el aviso de privacidad, así como limitarse a las finalidades que las justifiquen.

CAPÍTULO OCTAVO
VULNERACIONES DE SEGURIDAD

Artículo 38.- La vulneración a la seguridad de los datos personales se puede presentar en cualquier etapa del tratamiento (obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia, etc.).

Artículo 39.- Se entenderán como vulneraciones a la seguridad de los datos personales, al menos las siguientes:

I. Pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

Cuando se presente alguno de los supuestos antes descritos, existe la obligación del sujeto obligado de notificar en un **plazo máximo de 72 horas** a la o las personas titulares de los datos, al Instituto de Acceso a la Información Pública para el Estado de Guanajuato y a la Unidad de Transparencia del Municipio de León, Guanajuato las vulneraciones de seguridad ocurridas y que de alguna forma afecte los derechos patrimoniales o morales a los titulares de los datos personales.

Artículo 40. - La notificación deberá contener lo siguiente de acuerdo a la Ley:

I. Naturaleza del incidente;
II. Datos personales comprometidos;
III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde puede obtener mayor información al respecto.

Artículo 41. - Cuando exista la vulneración a la seguridad de los datos personales, se deberá analizar las causas por las cuales se presentó el incidente e implementar las acciones preventivas y correctivas necesarias para adecuar las medidas de seguridad para que eviten la reincidencia en la vulneración. Por lo que una vez realizado lo anterior se deberá realizar el llenado de la Bitácora de vulneración de seguridad que se adjunta a los presentes lineamientos como **anexo 3**.

Artículo 42.- En caso de que alguna persona externa o personal adscrito al IMMujeres vulnere alguna de las medidas de seguridad la persona enlace deberá realizar un acta circunstanciada de hechos, para documentar lo sucedido, así mismo se deberá notificar a la Contraloría Municipal sobre la vulneración ocurrida.

TRANSITORIOS

Primero. – Las presentes Políticas entrarán en vigor a partir de la aprobación del Consejo Directivo del IMMujeres.

Segundo. – Las presentes políticas serán actualizadas cuando surtan reformas a la normatividad aplicable.

Tercero. – Notifíquese las presentes Políticas al personal adscrito al Instituto Municipal de las Mujeres de León Guanajuato.

BIBLIOGRAFÍA

Congreso del Estado de Guanajuato. (2025). Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Guanajuato. (Última reforma publicada el 05 de diciembre de 2017). Periódico Oficial del Gobierno del Estado de Guanajuato.

Congreso del Estado de Guanajuato. (2025). Ley de Transparencia y Acceso a la Información Pública para el Estado de Guanajuato. (Última reforma publicada el 20 de noviembre de 2023). Periódico Oficial del Gobierno del Estado de Guanajuato.

Cámara de Diputados. (2025). Ley General de Protección de datos personales en posesión de sujetos obligados. (Nueva Ley publicada el 20 de marzo de 2025). Diario Oficial de la Federación.

Cámara de Diputados. (2025). Ley General de Transparencia y Acceso a la Información Pública. (Nueva Ley publicada el 20 de marzo de 2025). Diario Oficial de la Federación.

ANEXO 1

LEÓN AYUNTAMIENTO 2024-2027

Política de Escritorio Limpio

1. Definición de Escritorio Limpio

El "escritorio limpio" es un concepto que promueve el mantenimiento de un espacio de trabajo ordenado, libre de documentos, equipos o materiales innecesarios, con el objetivo de maximizar la productividad, la seguridad de la información y el bienestar general de los empleados.

---

2. Directrices Generales

Orden y Limpieza:

- Todos los elementos en el espacio de trabajo deben tener un propósito funcional.
- Al final de la jornada laboral, los empleados deberán dejar su escritorio limpio y organizado, con todos los documentos y materiales personales guardados de manera segura.

Seguridad de la Información:

- Todos los documentos sensibles o confidenciales deben ser almacenados de forma segura. Esto incluye el uso de archivadores con llave, carpetas de seguridad, o dispositivos de almacenamiento cifrados.
- Los documentos en papel deben ser triturados al final del uso, nunca dejados en el escritorio o en espacios comunes.
- En entornos digitales, los archivos de trabajo deben estar protegidos por contraseñas, y la computadora debe ser bloqueada cuando no esté en uso.

Tecnología y Equipos:

- Al concluir la jornada laboral, los equipos electrónicos como computadoras, teléfonos y otros dispositivos deben ser apagados o bloqueados, a menos que las actividades o demandas del área requieran lo contrario.
- Los cables deben ser organizados y gestionados para evitar desorden y posibles accidentes.

Material de Oficina:

- El material de oficina debe ser almacenado de manera ordenada en cajones o estantes. Solo los elementos esenciales deben estar sobre el escritorio.
- Los empleados deben evitar acumular material innecesario o personal en su lugar de trabajo.

3. **Beneficios del Escritorio Limpio**

- Seguridad: La protección de la información sensible es una prioridad, y mantener un escritorio limpio ayuda a evitar la exposición de documentos confidenciales.

- Productividad: Un espacio organizado permite a los empleados encontrar rápidamente lo que necesitan y centrarse en sus tareas sin distracciones innecesarias.

- Ambiente de Trabajo: Un entorno ordenado contribuye al bienestar y comodidad de todos los empleados, promoviendo un ambiente de trabajo profesional.

Aplicación y verificación del Documento de Seguridad en las Dependencias, Entidades y/o Órganos Autónomos, para garantizar las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

ANEXO 2

LEÓN AYUNTAMIENTO 2024-2027

Préstamo de Equipo de Computo

Por medio del presente, se hace constar que el(los) siguiente(s) equipo(s) de cómputo ha(n) sido entregado(s) en calidad de **préstamo temporal** al C. **(Nombre del servidor público)**, quien se desempeña como **(puesto del servidor público)** en el área de **(nombre del área)** de esta institución, para el desempeño de sus funciones laborales.

Detalles del equipo:

- **Tipo de equipo:**
- **Marca:**
- **Modelo:**
- **Número de serie:**
- **Inventario institucional:**

El préstamo es de carácter temporal y el servidor público se compromete a hacer uso adecuado del equipo, conservarlo en buen estado, y devolverlo en las mismas condiciones en que le fue entregado, salvo el desgaste natural por uso conforme a sus funciones.

El equipo permanecerá bajo su resguardo mientras dure la comisión o necesidad institucional que justifique su uso, y deberá ser devuelto en caso de baja, cambio de adscripción o cuando sea requerido por el área correspondiente.

Sin más por el momento, quedo atento(a) a cualquier comentario adicional.

Atentamente,
[Nombre del responsable del área que otorga el equipo]
[Cargo]
[Dependencia o unidad administrativa]
[Firma]

Recibí conforme:
C. [Nombre del servidor público]
[Cargo]
[Firma y fecha]

ANEXO 3

BITÁCORA DE VULNERACIONES DE SEGURIDAD				
Generales	Fecha	Día	Mes	Año
Área vulnerada:				
Fecha de vulneración:				
Tratamiento de datos personales vulnerado				
Clasificación de datos vulnerados				
Datos Personales vulnerado				
Entorno de la información vulnerada	Física			
	Red Interna			
	Red inalámbrica			
	Red de terceros			
	Internet			
Volumen de titulares				
Fecha y hora aproximada de la vulneración				
Tipo de vulneración	Pérdida o destrucción no autorizada			

	Robo, extravío o copia no autorizada			
	Uso, acceso o tratamiento no autorizado			
	Otro			
Motivos posibles o identificados de la vulneración				
Acciones preventivas realizadas por el área vulnerada a fin de cesar la vulneración				
Nombre y cargo del responsable del área vulnerada				
Nombre y cargo del responsable del sistema o base de datos personales vulnerado				
Nombre y cargo de los usuarios del sistema o base de datos personales vulnerado				
Nombre y cargo de quien reporta la vulneración al responsable del área				
Nombre del Titular de la Unidad de Transparencia				
Fecha y hora en la que el				

responsable del área vulnerada informa a la Unidad de transparencia				
Nombres y Cargos de los integrantes del Comité de Transparencia				
Fecha y hora en que se informó al comité de transparencia				
Fecha y hora en que se notificó a los titulares la vulneración ocurrida				
Recomendaciones y medidas que el titular podrá adoptar para proteger sus intereses				
Fecha y hora en que el Sujeto Obligado como responsable a través del Comité de Transparencia notificó al IACIP la vulneración ocurrida				
Acciones correctivas implementadas definitivamente				
Nombre y firma del responsable del área vulnerada				

Nombre y firma del responsable del sistema o base de datos personales vulnerado		
Nombre y firma de quien reporta la vulneración al responsable del área		
Nombre y firma del Titular de la Unidad de Transparencia		
Nombre y firmas de los integrantes del Comité de Transparencia		