GUÍA PARA EL TRATAMIENTO DE DOCUMENTOS QUE CONTIENEN

DATOS PERSONALES O INFORMACIÓN SENSIBLE

IEM
INSTITUTO ELECTORAL DE MICHOACÁN

La Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia a la Información Pública, así como las leyes locales en la materia, atribuyen a este Instituto Electoral de Michoacán, en cuanto sujeto obligado la facultad de generar instrumentos y herramientas que provean de certeza a la persona titular de los Datos Personales, de que éstos son tratados debidamente.[1]

Todo lo anterior **con sustento al derecho humano a la vida privada,** es decir, al derecho de no ser molestados por persona o entidad alguna, en las actividades que legítimamente decide mantener fuera del conocimiento público.

1De acuerdo con los artículos 3, fracción XXII, y 8 de la Ley General de Transparencia, Acceso a la Información y protección de datos personales del Estado de Michoacán de Ocampo, el Instituto es sujeto obligado a transparentar y permitir el acceso a la información y proteger los datos personales que obren en su poder, así como el artículo 2 en su fracción III, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán.

CONTACTO

Bruselas No. 118,
Col. Villa Universidad,
C.P. 58060, Morelia,
Michoacán, México.

Órgano Central:
(443) 322 1400
Transparencia:
(443) 322 1400 Ext. 1110

www.iem.org.mx

¿Qué son los
DATOS PERSONALES?

Ante esto, es importante definir que los Datos Personales son cualquier información concerniente a una persona física identificada o identificable, ya sea directa o indirectamente a través de cualquier información, como son los siguientes:

I. Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía y demás análogos;

II. Datos electrónicos: Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;

III. Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y análogos;

IV. Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos;

V. Datos judiciales o administrativos: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho;

¿Qué son los
DATOS PERSONALES?

VI. Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados, reconocimientos y demás análogos;

VII. Datos de tránsito y movimientos migratorios: Como es la ruta de tránsito, lugares donde se ha residido fuera del país, así como información migratoria;

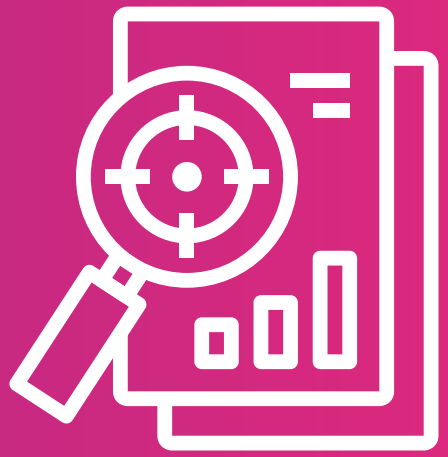
VIII. Datos sobre la salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona;

IX. Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos;

X. Datos especialmente protegidos (sensibles): origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas e identidad sexual; y aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

¿Qué son los
DATOS PERSONALES?

En virtud a que la norma que protege los derechos humanos tiene la tendencia a la evolución y la máxima garantía, **esta lista es enunciativa, no limitativa.**



Cotidianamente, en el desempeño de las atribuciones de este Instituto, las áreas que lo conforman están en contacto, tratamiento y almacenamiento de Datos Personales, y su procesamiento en cada una de éstas es distinto, por lo que generar homogeneidad en la forma de su recepción, tratamiento y protección es una forma útil de **cumplir con la disposición de protección de los Datos.**

De acuerdo con el **artículo 13 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo,** en la generación, publicación y entrega de información se deberá garantizar que ésta sea accesible, confiable, verificable, veraz, oportuna y atienda las necesidades del derecho de acceso a la información de toda persona, de modo que en el apartado siguiente se hacen una serie de propuestas para el cuidado de esta información.

De la

RECEPCIÓN DE DOCUMENTACIÓN

Siempre se tomará en cuenta que su recepción deberá cumplir con los principios destacados en el artículo 12 de la Ley de Protección de Datos en Posesión de Sujetos Obligados, los cuales son:

Licitud: Se recabarán de manera legal, sin engaños y por la vía oficial, de acuerdo con las facultades del Instituto.
Finalidad: Deberá dar a conocer los fines para los que se recaba la información y estas deberán ser legitimas, concretas y lícitas.
Lealtad: No se obtendrán Datos a través de medios engañosos o fraudulentos.
Consentimiento: Siempre se deberán recabar los Datos con autorización del titular, excepto en los casos que la ley señala claramente.
Calidad: Solo se requerirán los datos necesarios y se usarán exactamente para los dispuesto en los avisos de privacidad.
Proporcionalidad: Solo se tratarán los que sean necesarios para el trámite o actividad en concreto.
Información: Siempre y en todos el Instituto deberá dar a conocer cuál será el tratamiento de la información a la ciudadanía, a través de los avisos de privacidad que se encuentran en la página institucional Avisos de Privacidad (iem.org.mx)

Responsabilidad: El instituto deberá generar permanentemente mecanismos y prácticas que procuren la Protección de los Datos Personales, así como dar a conocer al titular de los Datos Personales, la forma en que pueden ejercer sus derechos ARCO.

Adicional a todo lo anterior, los responsables de la información deberán garantizar la accesibilidad, existencia y disponibilidad, señalando oportunamente los casos en los que no se cuenta con la información, a fin de realizar los procedimientos adecuados para la aprobación de la declaratoria de inexistencia de la misma, en su caso.

En el
TRATAMIENTO

Para el debido tratamiento de los Datos Personales, se propone que el Instituto a través de las áreas lo integran realicen las siguientes actividades:

1. Establecer criterios homogéneos para la asignación de nombres a documentos y expedientes. Se sugiere hacer listado mensual sobre aquellos expedientes que contienen datos personales para hacer del conocimiento a la Coordinación de Transparencia y Accesi a la Información.

2. Controles respecto del tratamiento de los Datos: Generar roles o determinar qué personas tratarán cada tipo de información, entre esta los Datos Personales.

3. Mantener los escritorios limpios: Mantener la información resguardada y ordenada en determinados espacios en los que solo una persona o las personas designadas puedan tener acceso a ellos.

4. Digitalización: la tendencia a digitalizar y usar menos papel es mayor y deberá tenerse debido cuidado al momento de la conservación de la información, eventualmente se promoverá el uso de nubes institucionales a fin de evitar el uso de medios de comunicación como correos electrónicos o dispositivos de carácter personal para el tratamiento, digitalización y almacenamiento de los datos personales.

5. Accesos restringidos: Se propone que se cambien las contraseñas al menos una vez al año, si se tiene la información almacenada en lugares físicos deberá gestionarse que estos puedan cerrarse con llave, candado o clave.

6. Capacitación permanente: Se invita a todo el personal, sobre todo aquellos vinculados con la Coordinación de Transparencia, tales como los enlaces de la misma a asistir a las reuniones que sean convocadas con la finalidad de actualizarse en la materia. (Se sugiere hacer capacitaciones seguidas a todo el personal que maneje o tenga en su poder datos personales)

7. Revisiones: realizar al menos cuatro veces al año una revisión respecto de los documentos que contengan Datos Personales, información reservada o sensible, que se conservan en el área, a fin de determinar si es susceptible de conservarse o bien a reconducirse al área responsable de su archivo.

8. En caso de robo o perdida de documentación importante, que contenga Datos Personales se deberá dar vista al superior jerárquico y a la Coordinación de Transparencia, para que ésta a través del Comité de Transparencia avale la inexistencia de la información.

En el
TRATAMIENTO

9. Evitar tirar documentos con información sensible o datos personales al bote de basura, ello no garantiza la secrecía a la cual se compromete el Instituto, respecto de este tipo de datos.

10. Cumplir con el Código de Ética elaborado por la Contraloría Interna de este órgano, así como a la Carta de compromiso de Confidencialidad que deberá estar integrada al expediente laboral de cada integrante del IEM.

11. Cuando los Datos personales hayan dejado de ser necesarios para la actividad o procedimiento que fueron recabados deberán ser testados y remitidos a los responsables de archivos, quienes ejecutarán los protocolos de destrucción adecuados.

12. Establecer periodos para su conservación, que se cumplan.

13. Guardar confidencialidad respecto de los datos personales, aun después de finalizar sus relaciones contractuales.

De la
DESTRUCCIÓN DE DOCUMENTOS QUE INTEGREN DATOS PERSONALES

Establecer criterios de almacenamiento con base en la clasificación de la información, es decir, si se trata de información sensible, datos personales o delicada debe resguardarse con niveles de seguridad mayores, tanto si se trata de documentos digitales como de papel.

Asimismo, su conservación, cuidado y tratamiento deberá ir de acuerdo con los valores primarios y secundarios de los documentos:

- PRIMARIOS: El valor que posee un documento en tanto es útil para el cumplimiento de las atribuciones del área y del Instituto.

Administrativo: Tiene valor legal, pero solo en el ámbito interno del Instituto mientras se da cumplimiento a las responsabilidades.

Legales: Tienen valor dentro y fuera del Instituto, como contratos y documentos que contengan disposiciones legales cumplimentadas.

Fiscales: Documentos que en su contenido expresan movimientos de dinero y son útiles para la comunicación con autoridades como hacienda, finanzas, entre otros.

Contables: En su contenido expresan movimientos de dinero y sirven para dar seguimiento a dichos temas al interior del Instituto.

Técnicos: Contienen información procedimental respecto del Instituto.

- SECUNDARIOS: Es el valor que adquieren los documentos una vez que pierden su valor primario.

Histórico: Permiten la reconstrucción de la memoria del Instituto.

Cultural: En su contenido se encuentran testimoniales, vivencias, tradiciones, valores y todos aquellos útiles para el reconocimiento de la identidad del IEM.

Científico: Documentos que contienen estudios e investigaciones en torno a los temas de interés del órgano administrativo electoral.

De la
DESTRUCCIÓN DE DOCUMENTOS QUE INTEGREN DATOS PERSONALES

En el caso concreto, y con independencia de las valoraciones de los documentos, se entiende que aquellos documentos que contienen Datos Personales e información sensible deberán ser conservados únicamente durante el periodo necesario para el cual fueron solicitados, para lo cual deberán señalarse siempre periodos o fechas de destrucción de la información específicas y/o medios de almacenamiento específicos.

Por otra parte, la información que sea clasificada como reservada e integrada al índice de información de información reservada, será mantenida en el archivo de concentración sin que pueda ser publicitada durante el periodo de clasificación, posteriormente podrá publicitarse u otorgarse a la ciudadanía previa solicitud de información y deberá seguir las medidas de conservación que se implementen para su almacenamiento seguro.

Esta última al tratarse de información de pudiera contener datos personales o no, toda vez que su reserva no atiende sólo a esta característica, una vez que deje la clasificación de reservada, será conservará los tiempos que en su momento se establezcan en los catálogos de disposición documental del área.

En todos y cada uno de los casos, una vez que se determine que la función del documento terminó, deberá integrarse a un inventario de documentos susceptibles de baja y serán remitidos al responsable de archivos, quien se encargará de su destrucción, procurando el cuidado de la información que contiene.

De las

SANCIONES

Debemos tener en cuenta que los Datos personales están al cuidado del Instituto, sin embargo, no nos pertenecen, y en todos los casos el titular de los mismos tiene el derecho de que sean protegidos y el Instituto la obligación de cumplir con esta disposición.

Por lo tanto, el o la ciudadana que considere que estos fueron vulnerados podrá presentar una queja ante el órgano garante, quien determinará si se incurre en alguna de las siguientes causas de responsabilidad:[2]

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables.
VII. Incumplir el deber de confidencialidad establecido en la presente Ley;
VIII. No establecer las medidas de seguridad en los términos establecidos en el Capítulo de los Deberes de la presente Ley;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad contempladas en la presente Ley;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;
XII. Crear bases de datos personales en contravención a lo dispuesto por la presente Ley;

En caso de acreditarse la falta, el IMAIP o el INAI determinarán cuál de las siguientes sanciones amerita el responsable:[3]

I. La amonestación pública;
II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y considerados en las evaluaciones que realicen éstos.

Es importante tomar medidas que permitan una recepción segura, un tratamiento y conservación adecuado al tipo de información con la que se trata y una destrucción de la información responsable.

---

[2] De acuerdo con el artículo 132 de la Ley de Protección de Datos en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo.
[3] Artículo 122, misma ley.