Programa de Protección de Datos Personales del Instituto de Investigaciones Dr. José María Luis Mora

Índice

Presentación **1**
Glosario **1**
1. Objetivo general **3**
2. Responsabilidades dentro del Programa **3**
3. Alcance del Programa **4**
4. Política de Gestión de Datos Personales **5**
4.1. Inventario de tratamiento 6
4.2. Avisos de Privacidad 9
4.3. Documento de Seguridad 10
5. Proceso de revisión y mejora continua **11**
6. Sanciones **18**

Presentación

El Instituto de Investigaciones Dr. José María Luis Mora es una entidad paraestatal, asimilada al régimen de organismos descentralizados según lo dispuesto en la Ley Orgánica de la Administración Pública Federal y la Ley Federal de las Entidades Paraestatales. Cuenta con el carácter de Centro Público, de acuerdo con los artículos 81 y 84 de la Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación, y está presupuestalmente sectorizado dentro del Ramo Administrativo 38: Humanidades, Ciencias, Tecnologías e Innovación, bajo la coordinación del Consejo Nacional de Humanidades, Ciencias y Tecnologías (Conahcyt).

Tiene la obligación de promover, respetar, proteger y garantizar los derechos humanos, conforme a los principios de universalidad, interdependencia, indivisibilidad y progresividad, así como de garantizar el respeto, la protección y la promoción de la igualdad.

En este sentido, el Comité de Transparencia del Instituto Mora está comprometido con la función de coordinar las acciones necesarias para dar cumplimiento a las disposiciones aplicables en materia de transparencia, acceso a la información y protección de datos personales.

El Programa de Protección de Datos Personales del Instituto Mora, en cumplimiento con lo establecido en el artículo 30 de la Ley General de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), fortalece el entramado normativo institucional con el objetivo de garantizar el tratamiento legal de los datos personales que se encuentran en su posesión.

El Programa se diseñó con la visión de servir como una guía para las personas servidoras públicas en el tratamiento de datos personales en el ejercicio de sus funciones y atribuciones. Por ello, dicho Programa está construido con base en un sistema de gestión para la protección de los datos personales, que proporciona los elementos y actividades de dirección, operación y control de los procesos del Instituto Mora, permitiendo proteger de manera sistemática y continua los datos. personales en su posesión, observando en todo momento los principios establecidos en el artículo 16 de la Ley en la materia.

Glosario

Área competente: Áreas administrativas a la que se le confieren atribuciones específicas en el Manual General de Procedimientos del Instituto de Investigaciones Dr. José María Luis Mora.

Auditoría voluntaria: Proceso sistemático, independiente y documentado mediante el cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) obtiene evidencias que le permiten evaluar el grado de cumplimiento en la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en las Leyes y demás normativa que resulte aplicable.

Aviso de Privacidad: Documento a disposición del titular de forma física, electrónica, o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física.

Catálogo de Disposición Documental: Instrumento archivístico a través del cual se establecen los criterios relativos a los valores documentales, plazos de conservación, vigencia documental, clasificación de reserva o confidencialidad y destino final de los expedientes generados en el ámbito administrativo y jurisdiccional, de acuerdo a las series documentales establecidas en el Cuadro General de Clasificación Archivística.

CGCA: Cuadro General de Clasificación Archivística que es el instrumento técnico para la identificación y agrupación de los expedientes en forma homogénea, de acuerdo a la estructura jerárquica y a las funciones del Instituto de Investigaciones Dr. José María Luis Mora.

Causas de no conformidad: Se entenderá por causas de no conformidad aquellos supuestos en los que el tratamiento de los datos personales realizado por las unidades competentes no cumpla con lo establecido en la normatividad aplicable, el Documento de Seguridad y este Programa.

Comité de Transparencia: Comité de Transparencia del Instituto Mora.

Datos personales: Cualquier 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.

Datos personales sensibles: 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. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, de conformidad con lo establecido en el Título Tercero de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Documento de Seguridad: Instrumento que describe y da cuenta de las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable.

Evaluación de impacto en la protección de datos personales: Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, puedan identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables.

Indicador: La variable o factor que proporciona un medio sencillo y fiable para medir logros, cambios o ayudar a evaluar resultados.

Inventario de tratamiento: Control documentado que se llevará de los tratamientos que realizan las áreas competentes del Instituto Mora, con orden y precisión.

Instituto Mora: Instituto de Investigaciones Dr. José María Luis Mora.

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos de Protección de Datos Personales en el Sector Público.

Programa: Programa de Protección de Datos Personales del Instituto de Investigaciones Dr. José María Luis Mora

Responsable: Sujeto obligado de la LGPDPPSO que decide el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada que se realiza con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Titular: Persona física a quien corresponden los datos personales.

Transferencia: Toda comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones afectadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidad de Transparencia: Cumple con lo establecido en el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

1. Objetivo general

El Programa de Protección de Datos Personales tiene como objetivo que el Instituto Mora garantice que el tratamiento de los datos personales en su posesión cumpla con los principios y obligaciones previstas en la LGPDPPSO y en los Lineamientos Generales.

Para lograrlo, se han establecido los siguientes objetivos:

- Proveer el marco de trabajo necesario para que el Instituto Mora cuente con los elementos suficientes que le permitan asegurar la efectividad de los procesos internos para el tratamiento y la seguridad de los datos personales en posesión de las áreas competentes. Estos procedimientos internos, en conjunto, constituyen el sistema de gestión para la protección de los datos personales.

- Asesorar y acompañar de manera constante y continua a los responsables y encargados del tratamiento de datos personales del Instituto Mora, a fin de garantizar que cumplan con el principio de responsabilidad.

- Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en el Instituto Mora, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

2. Responsabilidades dentro del Programa

De conformidad con lo dispuesto en los artículos 83 y 84, fracción I, de la LGPDPPSO y 47, segundo párrafo, y 48 de los Lineamientos Generales, el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y dentro de sus funciones se encuentra el coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el Instituto Mora. Por ello, dicho órgano colegiado tendrá, en relación con este programa, las funciones siguientes:

I. Aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar.

II. Proponer cambios y mejoras al Programa, a partir del informe anual que presentará la Unidad de Transparencia.

III. Dar a conocer el Programa al interior del sujeto obligado a través de la Unidad de Transparencia.

IV. Coordinar la implementación del Programa en las áreas competentes del Instituto Mora.

V. Asesorar a las áreas competentes en la implementación de este Programa, con el apoyo de la Unidad de Transparencia.

VI. Aprobar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y

VII. Las demás que de manera expresa señale el propio Programa.

El informe que la Unidad de Transparencia rendirá anualmente al Comité de Transparencia deberá presentarse a más tardar en la sesión ordinaria que se encuentre programada para el mes de junio de cada año. En caso de no existir una sesión ordinaria, se podrá presentar en sesión extraordinaria previa autorización del Presidente del Comité de Transparencia. El contenido del informe versará sobre las acciones instrumentadas y el seguimiento al cumplimiento del Programa en el año inmediato anterior, y reportará al menos:

- Información general sobre el cumplimiento de las obligaciones señaladas en el Programa por parte de las áreas competentes.
- Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Programa.
- Los resultados de las revisiones y/o auditorías realizadas; y
- Los incidentes que deriven de un posible tratamiento inadecuado de datos personales.

Para que los objetivos planteados se logren con éxito deberá ser notificado de forma directa a las personas titulares de las áreas competentes que integran el Instituto Mora.

En caso de que durante alguna de las revisiones o actualizaciones se determine que el Instituto Mora realiza algún tipo de tratamiento intensivo o relevante de datos de conformidad con lo establecido en el Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales1, la persona que ocupe la Dirección de Datos Personales asumirá las funciones del Oficial de Protección de Datos, previstas en los artículos 85 de la LGPDPPSO; y, 121 y 122 de los Lineamientos Generales.

3. Alcance del Programa

Este Programa es de observancia obligatoria para todas las personas servidoras públicas que en el ejercicio de sus funciones realicen el tratamiento de datos personales.

En este sentido, las distintas áreas competentes del Instituto Mora y la Unidad de Transparencia tendrán las funciones y responsabilidades que se describen a lo largo de este Programa, del Documento de Seguridad y de los inventarios actualizados. Por lo que las áreas competentes

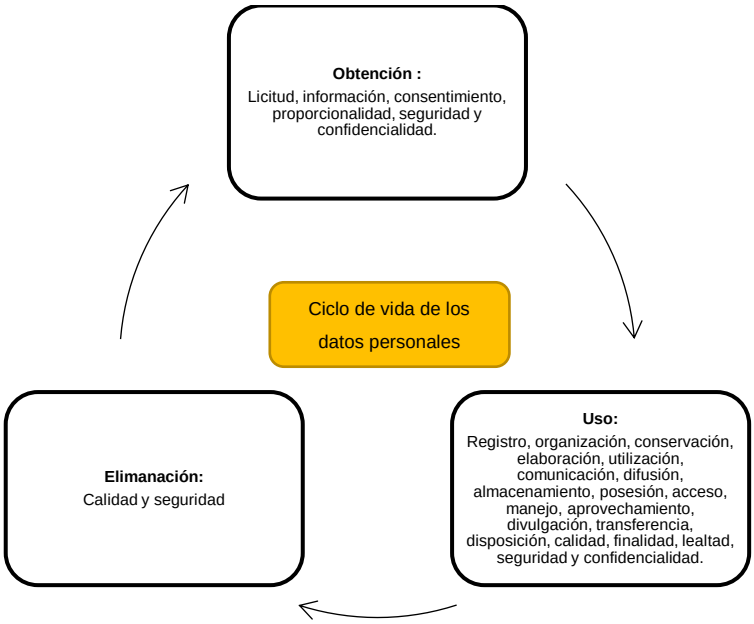
[1] Publicado en el Diario Oficial de la Federación, el primero de enero de dos mil dieciocho, disponible para consulta en: https://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018&print=true

deberán realizar las acciones necesarias para cumplir con las obligaciones que establecen dichos instrumentos, incluyendo la asignación de recursos materiales y humanos necesarios, así como la previsión de las metas y actividades que estimen necesarias dentro de sus respectivos programas de trabajo.

4. Política de Gestión de Datos Personales

Las áreas competentes del Instituto Mora que realicen el tratamiento de datos personales deberán cumplir con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales; así como con los deberes y obligaciones que prevé la LGPDPPSO, para lo cual este Programa establece el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las áreas competentes, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales en concordancia con el ciclo de vida de los datos personales. (ver la siguiente imagen):



Durante el ciclo de vida de los datos personales, el Instituto Mora deberá contar con las versiones actualizadas de los inventarios de sistemas de tratamiento, avisos de privacidad simplificados e integrales y con el documento de seguridad institucional; documentos a través de los cuales se deberá garantizar el cumplimiento de los siguientes principios:

Principio de licitud: el tratamiento de los datos personales será exclusivo de las facultades del responsable.

Principio de finalidad: las finalidades del tratamiento de los datos personales deberán ser concretas a fin de no generar incertidumbre a las personas titulares de los datos personales; explícitas de modo que brinden claridad, acordes con los avisos de privacidad; lícitas al ser acordes con las atribuciones del responsable; y legítimas por contar con el consentimiento del titular de los datos. En el caso de que se requiera hacer un tratamiento distinto al de la finalidad para la cual se recabaron los datos personales se deberá considerar la expectativa razonable de privacidad de la persona titular basada en la relación que tiene con éste; la

naturaleza de los datos; las consecuencias del tratamiento posterior de los datos personales para el titular, y las medidas adoptadas para que el tratamiento posterior cumpla con las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales.

Principio de lealtad: los datos personales no se deberán recabar por medios engañosos o fraudulentos; se privilegiarán los intereses de la persona titular para no dar lugar a discriminación o trato injusto; todos los datos personales recabados deberán de ser tratados conforme a lo señalado en los avisos de privacidad.

Principio de consentimiento: ser recabará el consentimiento del titular, de manera libre, especifica e informada.

Principio de calidad: los datos personales deberán ser exactos y correctos, completos, actualizados.

Principio de proporcionalidad: los datos recabados deberán de ser estrictamente los necesarios, apropiados e indispensables y no excesivos para el cumplimiento de las finalidades.

Principio de información: se deberán comunicar, por medio del aviso de privacidad, las características de los tratamientos a los que se someterán los datos personales.

Principio de responsabilidad: adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la LGPDPPSO.

A continuación, se especifican los contenidos mínimos de cada uno de los documentos anteriormente referidos:

4.1. Inventario de tratamiento

Para poder verificar el cumplimiento de las obligaciones previstas en el artículo 35, fracción I, de la LGPDPPSO, es necesario contar con un diagnóstico de cada uno de los procesos que involucran tratamiento de datos personales. Este diagnóstico se realiza a través de la elaboración de un "inventario de tratamiento" de datos personales, el cual debe formar parte del documento de seguridad.

Para garantizar orden y precisión en los inventarios, se deben tener en consideración los elementos mínimos establecidos en los artículos 58 y 59 de los Lineamientos Generales de Datos:

> ***"Inventario de datos personales***
>
> ***Artículo 58.*** *Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*
>
> *I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*
>
> *II. Las finalidades de cada tratamiento de datos personales;*
>
> *III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*
>
> *IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*

V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;

VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Ciclo de vida de los datos personales en el inventario de éstos

Artículo 59. *Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:*

I. La obtención de los datos personales;

II. El almacenamiento de los datos personales;

III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;

IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;

V. El bloqueo de los datos personales, en su caso, y

VI. La cancelación, supresión o destrucción de los datos personales.

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar. "

A partir de ello y como parte del proceso de mejora continua, la Unidad de Transparencia realizó, en coordinación con las áreas competentes, la revisión y homologación de los inventarios de tratamiento de datos personales referidos en el Documento de Seguridad, conforme al diseño propuesto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en el "Programa de Protección de Datos. Documento Orientador". Actualmente, el Documento de Seguridad del Instituto Mora, documenta la existencia de inventarios de tratamiento de datos personales.

En este sentido, y considerando la posibilidad de identificación de nuevos tratamientos o la actualización de los inventarios vigentes, las áreas competentes deberán remitir un oficio con los ajustes requeridos a la Unidad de Transparencia y el formato de inventario actualizado, para que la Unidad de Transparencia realice las sugerencias que considere pertinentes, a fin de verificar el apego a los principios y deberes normativamente establecidos.

El formato en Excel mencionado contiene los siguientes apartados (ver imagen)

Formato de inventarios de tratamiento de datos personales del Instituto de Investigaciones Dr. José María Luis Mora

Unidad administrativa:	Señalar nombre de la unidad administrativa a cargo o administradora del proceso o procedimiento en el que se tratan los datos personales.
Fecha de elaboración o última actualización:	Señalar fecha en la que concluyó la elaboración del inventario o su última actualización
Nombre del tratamiento (proceso):	Señalar nombre del tratamiento.
Fundamento jurídico que habilita el tratamiento:	Señalar las principales disposiciones normativas, artículos, apartados, fracciones, incisos, párrafos de los que deriva el tratamiento en cuestión.
Atribuciones de la unidad administrativa para realizar el tratamiento:	Señalar las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento, entre ellas, las que señala el Reglamento o Estatuto Orgánico interno,

Medio de obtención de los datos personales (1)			Tercero que transfiere los datos personales, en su caso (2)	Finalidades de la transferencia recibida, en su caso (3)
Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, se deberá indicar un medio por fila.	Describir el medio, por ejemplo la fuente de acceso público, URL, domicilio, número telefónico, entre otros	En caso de seleccionar la opción otro, especificar el medio de obtención.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del tercero o terceros que realizan la transferencia.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidades se realiza dicha transferencia. Se deberá utilizar la misma fila por tercero que transfiere los datos personales.

Listado de datos personales (4)		Sensible (5)	Formato de la base de datos (6)	Ubicación base de datos (7)		Sección de archivos (8)	Serie de archivos (9)
Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	En caso de seleccionar la opción otro, especificar.	Señalar si el dato personal es sensible o no.	Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.	Señalar la ubicación de la base de datos. Si es más de uno, se deberá indicar uno por fila.	En caso de seleccionar la opción otro, especificar la ubicación.	Indicar clave de identificación de la sección a la que corresponde el tratamiento.	Indicar clave de identificación de la serie a la que corresponde el tratamiento.

Subserie de archivos (10)	Finalidades del tratamiento (11)	¿Requiere consentimiento? (12)	Supuesto artículo 22 que se actualiza, en su caso (13)	Tipo de consentimiento (14)	Servidores públicos que tienen acceso a la base de datos (15)	Área de adscripción (16)
Indicar clave de identificación de la subserie a la que corresponde el tratamiento.	Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una por fila.	Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad no requiera el consentimiento del titular, señalar el o los supuestos del artículo 22 de la LGPDPPSO que se actualizan.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.	Señalar los puestos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.	Definir unidad administrativa a la que está adscrito el puesto

Finalidad del acceso (17)	Nombre del encargado, en su caso (18)	No. de contrato, pedido o convenio con el encargado, o del instrumeto juridico correspondiente (19)	¿Se realizan transferencias? (20)	Tercero al que se transfieren los datos personales, en su caso (21)	Finalidades de la transferencia (22)	¿Requiere consentimiento la transferencia? (23)	Supuestos articulos 22, 66 o 70 que se actualizan, en su caso (24)
Señalar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.	Señalar nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso. Uno por fila.	Señalar el número de identificación del instrumento jurídico que regula la relación con el encargado.	Señalar si se realizan o no transferencias en el marco del tratamiento.	Señalar el nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, cuando ello sea posible, o bien, su categoría. Uno por fila.	Señalar las finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.	Señalar si la transferencia requiere o no consentimiento.	En caso de que la transferencia no requiera consentimiento, señalar los supuestos que se actualizan.

Tipo de consentimiento que se requiere para la transferencia (25)	¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico? (26)	Supuesto artículo 66 que se actualiza, en su caso (27)	Difusión de los datos personales (28)	Fundamento jurídico para la difusión (29)	Plazo de conservación (30)	Bloqueo (31)	Observaciones
En caso de que la finalidad de la transferencia requiera el consentimiento del titular, señalar si se requiere el tácito o el expreso y por escrito.	Indicar si la transferencia requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, según el artículo 66 de la LGPDPPSO.	Señalar el supuesto que en su caso se actualiza, si no se requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico.	Indicar si en el tratamiento se realiza la difusión de los datos personales.	Indicar el fundamento jurídico que ordena la difusión de los datos personales.	Señalar el plazo de conservación de los datos personales, según lo señalado en los instrumentos de clasificación archivística.	Señalar periodo en el que estarán bloquedos los datos personales.	Espacio libre para hacer aclaraciones y precisiones

4.2. Avisos de Privacidad

De conformidad con los artículos 3, fracción II, 18, 26 y 27 de la LGPDPPSO, 26, 27 y 28 de los Lineamientos Generales; cada sistema de tratamiento de datos personales del Instituto Mora debe contar con un aviso de privacidad integral y uno simplificado. Estos avisos deben hacerse del conocimiento de las personas titulares de los datos personales de forma previa a recabar los datos, por lo que las áreas competentes deben contar con ejemplares impresos, con independencia de que en el portal de internet del Instituto Mora se encuentren disponibles para garantizar que cualquier persona pueda consultarlos.

Los avisos de privacidad integrales deberán contar, cuando menos, con los elementos siguientes:

1. El domicilio del responsable.
2. Los datos personales que serán sometidos a tratamiento, identificando aquellos que son sensibles.
3. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento.
4. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento de la persona titular.
5. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO.
6. El domicilio de la Unidad de Transparencia; y
7. Los medios a través de los cuales el responsable comunicará a las personas titulares de los cambios al aviso de privacidad.

Los avisos de privacidad simplificados deberán contar con, al menos, los elementos siguientes:

1. La denominación del responsable.

2. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento de la persona titular.

3. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar.

a Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales.

b Las finalidades de estas transferencias.

4. Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular; y

5. El sitio donde se podrá consultar el aviso de privacidad integral.

Cuando un área competente cree o actualice su aviso de privacidad, por medio de oficio deberá de hacerlo del conocimiento de la Unidad de Transparencia para que pueda dar seguimiento y verificar que cumplan con las obligaciones previstas en la normatividad aplicable y que se haya actualizado en el portal de internet del Instituto Mora.

En caso de que se requieran precisiones o ajustes al respecto, la Unidad de Transparencia lo hará del conocimiento del área competente y proporcionará la asesoría y acompañamiento necesario.

Actualmente, los avisos de privacidad tanto integrales como simplificados se encuentran disponibles en: https://www.institutomora.edu.mx/Instituto/SitePages/AP.aspx

4.3. Documento de Seguridad

En cumplimiento de las obligaciones de seguridad, el nueve de abril de dos mil veinticuatro, el Comité de Transparencia aprobó la actualización al Documento de Seguridad del Instituto Mota; el cual, en cumplimiento al artículo 35 de la LGPDPPSO, contiene los apartados y anexos siguientes:

I-Presentación
II-Marco legal
III-Glosario
IV-Aplicabilidad
V-Estructura del documento de seguridad
  a) Inventario de datos personales y los sistemas de tratamiento.
  b) Medidas de Seguridad del Instituto Mora
  c) Análisis de riesgos
  d) Análisis de brecha
  e) Plan de trabajo
  f) Mecanismos de monitorio y revisión de las medidas de seguridad
  g) Programa de capacitación
  h) Actualización del documento de seguridad
VI. Aprobación del Documento de Seguridad del Instituto Mora.
-Anexo General

Sin embargo, este documento debe ser revisado al menos una vez al año y actualizarse cuando se presente alguno de los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión para la protección de los datos personales.
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; y
- Cuando se implementen acciones correctivas y preventivas ante una vulneración de seguridad.

En este sentido, al menos una vez al año, la Unidad de Transparencia deberá revisar el Documento de Seguridad. Durante esta revisión, se verificará que el documento incorpore todos los cambios o actualizaciones notificados por las áreas competentes. La Unidad de Transparencia solicitará la colaboración de las áreas competentes que hayan creado o modificado inventarios de datos personales, para elaborar la propuesta de actualización que se presentará al Comité de Transparencia para su revisión y, en su caso, aprobación.

5. Proceso de revisión y mejora continua

El proceso de revisión y mejora continua permitirá verificar que los parámetros establecidos en la LGPDPPSO, en los Lineamientos Generales, en este Programa de Protección de Datos Personales y en el Documento de Seguridad se cumplan cabalmente o permitan realizar los ajustes necesarios para su cumplimiento. La finalidad de la implementación cíclica de estas etapas permitirá garantizar el tratamiento óptimo de los datos personales en posesión del Instituto Mora y, en su caso, la posibilidad de solicitar una auditoría voluntaria al INAI en términos del artículo 151 de la LGPDPPSO.

Con ese fin, se establecen tres etapas cíclicas de trabajo:

ETAPA 1. Revisión de inventarios de datos personales y avisos de privacidad.

Con la finalidad de cumplir con la política de gestión de datos personales, las obligaciones y las verificaciones del Programa se llevará a cabo un análisis de los inventarios de datos personales y avisos de privacidad. Esta revisión permitirá verificar que se cumplen con las obligaciones normativas.

Objetivo	Actualización de inventarios y avisos de privacidad.
Nombre	Acompañamiento para actualizar inventarios y avisos de privacidad, en las áreas que realizan tratamiento de datos personales.
Método de cálculo	Número de sistemas reportados en la primera revisión x100 / Número de sistemas identificados en la segunda revisión.
Unidad de medida	Porcentaje.
Frecuencia de medición	Anual.
Tipo	Estratégico.
Dimensión	Eficacia.
Meta	Todas las áreas que realizan tratamiento de datos personales deberán contar con el inventario de datos personales y avisos de privacidad.

Medios de verificación	• Minutas de trabajo, oficios, correos electrónicos institucionales. • Avisos de Privacidad en la página de Transparencia (Apartado "Protección de datos personales, en términos del artículo 29 de los Lineamientos Generales). • Inventarios de datos verificados por la Unidad de Transparencia.

Objetivo	Elaboración de inventarios y avisos de privacidad.
Nombre	Acompañamiento para elaborar inventarios y avisos de privacidad, en las áreas que realizan tratamiento de datos personales.
Método de cálculo	Cantidad de áreas capacitadas o acompañadas para la elaboración de inventarios y avisos de privacidad/ Cantidad de áreas que ya cuentan con elaboración de inventarios y avisos de privacidad x 100.
Unidad de medida	Porcentaje.
Frecuencia de medición	Anual.
Tipo	Estratégico.
Dimensión	Eficacia.
Meta	Todas las áreas que realizan tratamiento de datos personales deberán contar con el inventario de datos personales y avisos de privacidad.
Medios de verificación	• Minutas de trabajo, oficios. • Avisos de Privacidad en la página de Transparencia (Apartado "Protección de datos personales, en términos del artículo 29 de los Lineamientos Generales). • Inventarios de datos verificados por la Dirección de Datos Personales.

ETAPA 2. Programa General de Capacitación. Instrumento mencionado en el Documento de Seguridad, cuyo diseño deberá comprender la implementación de talleres y asesorías especializadas dirigidas a las personas servidoras públicas que realizan algún tratamiento de datos personales. Este acompañamiento atenderá las necesidades detectadas por las propias áreas competentes, la Unidad de Transparencia y el Comité de Transparencia.

En estos espacios se orientará sobre la necesidad de implementar acciones preventivas; para ello, se realizarán las siguientes actividades:

El análisis y revisión de las posibles causas de no conformidad.

- Determinar las no conformidades que podrían desencadenarse, a partir de ciertas situaciones de riesgo para el tratamiento de datos personales.
- Evaluar las acciones necesarias para evitar que la no conformidad ocurra.
- Determinar e implementar estas acciones.
- Documentar los resultados de las acciones tomadas.
- Revisar la eficacia de las acciones preventivas tomadas.

Cuando se detecte la necesidad de implementar acciones correctivas encaminadas a eliminar las causas de la "no conformidad" o reducir su grado de prevalencia, la Dirección de Datos Personales lo comunicará al área competente y al Comité de Transparencia. Este último establecerá un plazo límite para que se solventen las no conformidades detectadas.
Las actividades vinculadas con las acciones correctivas deberán ser al menos las siguientes:

- Analizar y revisar la no conformidad.
- Determinar las causas que dieron origen a la no conformidad.

- Evaluar las acciones necesarias para evitar que la no conformidad vuelva a ocurrir.
- Implementar estas acciones.
- Documentar los resultados de las acciones tomadas.
- Revisar la eficacia de las acciones correctivas implementadas.

Objetivo	Que todas las personas servidoras públicas que tratan datos personales se encuentren capacitados en materia de protección de datos personales.
Nombre	Protección de datos personales.
Método de cálculo	Cantidad personal capacitado/ Cantidad de personal en proceso de capacitación x 100.
Unidad de medida	Porcentaje.
Frecuencia de medición	Anual.
Tipo	Estratégico.
Dimensión	Eficacia.
Meta	Todo el personal que realice atención a solicitudes ARCO deberá estar capacitado.
Medios de verificación	Constancias de capacitación de los cursos impartidos.

Objetivo	Que todas las personas servidoras públicas encargadas de dar trámite a solicitudes de ARCO, se encuentren capacitados en estos procedimientos de autodeterminación informativa.
Nombre	Autodeterminación informativa.
Método de cálculo	Cantidad personal capacitado/ Cantidad de personal en proceso de capacitación x 100.
Unidad de medida	Porcentaje.
Frecuencia de medición	Anual.
Tipo	Estratégico.
Dimensión	Eficacia.
Meta	Todo el personal que realice atención a solicitudes ARCO deberá estar capacitado.
Medios de verificación	Constancias de capacitación de los cursos impartidos.

ETAPA 3. Revisión y, en su caso, actualización del Documento de Seguridad. Cada año o cuando se detecte la creación o modificación de un inventario de tratamiento, se deberá actualizar dicho documento. Las necesidades generales de capacitación reportadas en el Documento de Seguridad se harán del conocimiento de la Unidad de Transparencia para que sean incorporadas en el Programa Anual de Capacitación que presenta ante el Comité de Transparencia.

Objetivo	Todas las áreas competentes que hacen uso de datos personales mantengan sus archivos tanto físicos como electrónicos e instalaciones debidamente resguardadas y habilitadas para evitar riesgos y vulneraciones de los datos personales que tienen bajo su resguardo.
Nombre	Evaluación de riesgos y vulneraciones en materia de datos personales.
Método de cálculo	Cantidad de áreas que verificaron riesgos. / Cantidad de áreas que cumplen con lo señalado en la ley de la materia para evitar riesgos y vulneraciones x 100.
Unidad de medida	Porcentaje.
Frecuencia de medición	Bianual.
Tipo	Estratégico
Dimensión	Eficacia
Meta	Todas las áreas que hacen uso de datos personales deberán cumplir lo dispuesto en la LGPDPPSO, generar registros de las personas servidoras públicas que tengan acceso a datos personales, así como cumplir con las medidas de seguridad señalas en la ley de la materia.
Medios de verificación	Registro de vulneraciones, minutas de trabajo, material fotográfico de las instalaciones u oficinas que dan tratamiento a datos personales (sin personas servidoras públicas), bitácoras de acceso o registro de cada servidora o servidor públicos que consulte o tenga acceso a datos personales.

Como parte de los insumos para llevar a cabo la revisión del Documento de Seguridad, y mientras no se apruebe o implemente algún formato o procedimiento por parte de las áreas competentes especializadas vinculadas con la seguridad física y técnica del Instituto Mora, se utilizarán los siguientes formatos para actualizar el análisis de riesgos y establecer la estrategia para reducir la frecuencia de las vulnerabilidades que se presentan.

Actualización de medidas de seguridad (Formato 1)

En cumplimiento con los artículos 31 y 32 de la LGPDPPSO y con el objeto de registrar las vulnerabilidades que se presentan, cada área responsable del tratamiento de datos personales deberá implementar la siguiente bitácora:

Sistema:	*Señalar el nombre del sistema de tratamiento de datos personales respecto del cual se actualizan las medidas de seguridad implementadas.*
Medios de conservación:	*Precisar si los datos personales se encuentran en soporte físico o electrónico.*
Medidas de seguridad administrativas:	*Indicar si cuenta con políticas y/o procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal en materia de protección de datos personales. (Si cuentan con algún protocolo interno implementado, clasificación y control de*

	archivos) En caso de contar con normativa específica, favor de adjuntarla.
SOPORTES FÍSICOS ***Son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento (archiveros, oficinas e instalaciones).***	
Tipos de soportes:	*Describir los soportes físicos (son expedientes, carpetas, etc.).*
Características del lugar de resguardo:	*Describir e incluir evidencia fotográfica de las características del lugar donde se resguardan dichos soportes (archiveros, gavetas, oficinas, edificios, instalaciones, etc.).*
Medidas de seguridad:	*Describir las medidas de seguridad (cerraduras, controles de acceso, bitácoras de acceso, etc.).*
SOPORTES TÉCNICOS ***Son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento (contraseñas, uso de VPN, discos duros, carpetas en*** *servidor con controles de acceso, correos electrónicos, micrositios).*	
Tipos de soportes:	*Describir los soportes electrónicos (discos duros, USB, servidor, equipos de cómputo, correos electrónicos, etc.).*
Características del lugar de resguardo:	*En el caso discos duros, USB, servidor, equipos de cómputo, describir cómo se resguardan o qué medidas se implementan para evitar su vulneración, pérdida o robo.*
Medidas de seguridad:	*Describir las medidas de seguridad implementadas (contraseñas, uso de VPN, discos duros, carpetas en servidor con controles de acceso, correos electrónicos, micrositios).*
TRANSFERENCIAS	
Medidas de seguridad al realizar transferencias:	*En caso de realizar transferencias, especifique por qué medio o medios las realiza y las medidas se seguridad que implementa para evitar la vulneración de los datos personales durante la transferencia. Describir las medidas de seguridad que implementa durante el envío (o traslado) de la información. (Por ejemplo: envío físico en sobres sellados verificando que se entregue a persona autorizada, envío electrónico en archivo que sólo se puede abrir con una contraseña o a través de alguna plataforma informática que garantice la seguridad de los datos, si existe algún control respecto de qué personas físicas realizan el traslado de los soportes).*
Enlace:	*Nombre del encargado*

Riesgo que generó alguna vulneración a los soportes en que resguarda los datos personales sometidos a tratamiento.	SI	NO
Abuso de privilegios de acceso		
Acceso no autorizado		
Alteración de la información		
Caída del sistema por sobrecarga		
Condiciones inadecuadas de temperatura o humedad		
Corrupción de la información		
Corte del suministro eléctrico		
Daños por agua		
Degradación de los soportes de almacenamiento de la información		
Denegación de servicio		
Desastres industriales		
Desastres naturales		
Destrucción de información		
Difusión de software dañino		
Errores de configuración		
Errores de los usuarios		
Errores de mantenimiento / actualización de equipos (hardware)		
Errores de mantenimiento / actualización de programas (software)		
Errores del administrador		
Extorsión		
Fallo de servicios de comunicaciones		
Fuego		
Fuga de información		
Indisponibilidad del personal		
Ingeniería social		
Interceptación de información (escucha)		
Interrupción de otros servicios y suministros esenciales		
Introducción de falsa información		
Pérdida de equipos		
Robo		

Formato de identificación de incidentes
(Formato 2)

En cumplimiento con el artículo 39 de la LGPDPPSO y con el objeto de registrar las vulneraciones que se presenten, cada área responsable de tratamiento de datos personales deberá implementar el registro siguiente:

INFORMACIÓN GENERAL (para ser llenado por quien detecta el incidente)					
Información del personal que detecta el incidente					
Nombre					
Dirección					
Teléfono y extensión		**Correo electrónico**		**Celular**	
Información sobre el incidente					
Fecha:		**Hora:**			
Localización donde se detectó el incidente					
Tipo de sistema de tratamiento		**Físico**		**Electrónico**	
Nombre del responsable del sistema de tratamiento					
Se encuentran involucrados datos personales		**Sí**		**No**	
Tipos de datos personales involucrados					
Descripción de lo sucedido					
Evaluación (para ser llenado por detecto el incidente)					
Una vez analizada la información, se determina que se trata de un incidente de seguridad		**Sí**		**No**	
Justificación					
Mencionar si existe algún posible impacto legal o contractual por el incidente:					
Nombre y firma de quien detecta el incidente			**Nombre y firma del titular del área**		

Este formato se deberá notificar directamente a la Unidad de Transparencia y a las áreas competentes al interior del Instituto Mora.

Adicionalmente, la Unidad de Transparencia deberá notificar el incidente a la persona titular de los datos personales y al INAI través del medio más inmediato, ya sea por teléfono, correo electrónico, correo postal o si es posible en persona, en los términos que a continuación se describen.

La notificación al INAI deberá contener al menos lo siguiente:

a) La hora y fecha en que se identificó la vulneración;
b) La hora y fecha en que inició la investigación sobre la vulneración;
c) La naturaleza de la vulneración ocurrida;
d) La descripción detallada de cómo ocurrió la vulneración;
e) Los tipos de datos personales comprometidos y el número aproximado de las personas titulares afectadas;
f) Los sistemas de tratamiento comprometidos;
g) Las acciones correctivas realizadas de forma inmediata;
h) La descripción de las posibles consecuencias de la vulneración ocurrida;
i) Las recomendaciones dirigidas a la persona titular;
j) El medio puesto a disposición del titular para que obtenga más información sobre la vulneración y cómo proteger sus datos personales;
k) El nombre completo de la o las personas designadas para proporcionar mayor información al INAI en caso de requerirse, y;
l) Cualquier otra información o documentación que considere conveniente hacer del conocimiento del INAI. En algunos casos, puede ser conveniente notificar a aseguradoras, instituciones financieras, autoridades de impartición de justicia o a centros de respuesta a incidentes, para obtener asesoría o proporcionar a los titulares mayor apoyo.

A las personas titulares se deberá notificar lo siguiente:

a) **Descripción de la vulneración:** Se debe explicar de manera muy sencilla y general el incidente ocurrido, en qué consistió, así como el periodo en el que se desarrolló. No se deben dar detalles o incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.
b) **Datos personales involucrados:** Una descripción de la información involucrada en el incidente.
c) **Recomendaciones a las personas titulares:** El listado de acciones que puede realizar la persona titular para minimizar los efectos adversos de la vulneración.
d) **Acciones correctivas o de mitigación:** Una descripción general de las acciones llevadas a cabo para evitar que se repitan incidentes similares.
e) **Información de contacto:** Datos de las áreas designadas, mesas de servicio o del personal de la organización que puede atender dudas y proporcionar información adicional del incidente.
f) **Fuentes de información adicional:** Referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad, en su caso.

6. Sanciones

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar un exhorto al área correspondiente para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.

II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.

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 LGPDPPSO.

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la LGPDPPSO, 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. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO.

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO.

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO.

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO.

XI. Obstruir los actos de verificación de la autoridad.

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO.

XIII. No acatar las resoluciones emitidas por el Instituto; y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII y XIV, así como la reincidencia en las conductas mencionadas en el resto de las fracciones, serán consideradas como graves.

De conformidad con el artículo 105 de los Lineamientos Generales, cuando algún área competente se niegue a colaborar con la Unidad de Transparencia en la atención de las

solicitudes para el ejercicio de los derechos ARCO, se dará aviso al superior jerárquico para que ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo notificará al Comité de Transparencia.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos. Las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se pueda derivar de los mismos hechos.

El Comité de Transparencia tomará las medidas necesarias para que las personas servidoras públicas del Instituto Mora conozcan esta información