Políticas internas para la gestión y el tratamiento de los datos personales en posesión del Instituto de Investigaciones Dr. José María Luis Mora

ÍNDICE

PRESENTACIÓN 1
OBJETIVOS 2
TÍTULO PRIMERO 3
Disposiciones Generales 3
TÍTULO SEGUNDO 8
Principios y deberes previstos en la Ley General y los Lineamientos Generales 8
CAPÍTULO I 8
De los principios 8
CAPÍTULO II 17
De los deberes 17
TÍTULO TERCERO 21
Obligaciones previstas en la Ley General y los Lineamientos Generales 21
CAPÍTULO I 21
De las transferencias y remisiones 21
CAPÍTULO II 25
De las mejores prácticas y evaluaciones de impacto 25
CAPÍTULO III 25
Del Programa de Protección de Datos Personales 25
CAPÍTULO IV 26
Del Documento de seguridad 26
CAPÍTULO V 29
Del proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad 29
CAPÍTULO VI 30
Del Programa de capacitación 30
CAPÍTULO VII 30
De la portabilidad 30
CAPÍTULO VIII 30
de datos personales 30
CAPÍTULO IX 31
Del ciclo de vida de los datos personales 31
TÍTULO CUARTO 33
Derechos ARCO 33
CAPÍTULO I 33
Del procedimiento para el ejercicio de los Derechos ARCO 33
CAPÍTULO II 37
Del Recurso de Revisión 37
TÍTULO QUINTO 38
De las sanciones 38
TRANSITORIOS 39

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 el artículo 84 de la Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación, y presupuestado aprobado al 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 ese contexto, es de vital importancia que el Instituto realice un tratamiento adecuado de los datos personales que se encuentran en su posesión, conforme a los términos y excepciones fijados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General) y demás normas aplicables.

Para lograr este objetivo, y en apego a lo previsto por los artículos 33, fracción I, de la Ley General y 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), que prevén la creación de políticas que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, se emiten estas políticas internas para la gestión y el tratamiento de los datos personales en posesión del Instituto de Investigaciones Dr. José María Luis Mora .

Este documento prevé actividades generales y mecanismos para el cumplimiento de los principios, deberes, derechos y obligaciones en materia de datos personales, de conformidad con lo previsto en la Ley General y en los Lineamientos Generales. También define los roles y responsabilidades de los involucrados en los tratamientos de datos personales efectuados por el Instituto, los rubros relacionados con las sanciones en caso de incumplimiento, el ciclo de vida de los datos personales sujetos a tratamiento, y el proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad. Asimismo, se contemplan los procesos generales de atención de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales en su posesión y del recurso de revisión.

OBJETIVOS

Objetivo General

Contar con un instrumento que articule y fortalezca el marco normativo institucional del Instituto de Investigaciones Dr. José María Luis Mora en materia de datos personales. Este instrumento servirá como guía para las áreas administrativas en el tratamiento de los datos personales en su posesión, permitiendo su protección de manera sistemática y continua, observando en todo momento los principios establecidos en el artículo 16 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Objetivos Específicos

Los objetivos específicos que se esperan lograr con la implementación de estas Políticas son:

- Establecer un sistema de gestión de los datos personales que asegure su protección y correcta administración.
- Definir las acciones generales que deben llevar a cabo las áreas administrativas del Instituto Mora para cumplir con los principios y deberes en materia de protección, tratamiento y conservación de los datos personales.
- Difundir internamente las directrices y criterios generales relacionados con el procedimiento de atención a solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales en su posesión.
- Garantizar la concordancia, cohesión, integración y relación con el Programa de Datos Personales, el Programa Anual de Capacitación en materia de Datos Personales y el Documento de Seguridad del Instituto de Investigaciones Dr. José María Luis Mora.

MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Archivos.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Ley General de Responsabilidades Administrativas
- Políticas de Seguridad de la Información y Objetivos del Instituto de Investigaciones Dr. José María Luis Mora.

ÁMBITO DE APLICACIÓN

Las Políticas son de aplicación y observancia general y obligatoria para todas las personas servidoras públicas del Instituto de Investigaciones Dr. José María Luis Mora, quienes, conforme a sus atribuciones, realicen el tratamiento de datos personales en posesión de este Instituto o tengan conocimiento de dichos datos por alguna circunstancia. Esto se establece en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales y demás normas aplicables en la materia.

POLÍTICAS INTERNAS PARA LA GESTIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES EN POSESIÓN DEL INSTITUTO DE INVESTIGACIONES DR. JOSÉ MARÍA LUIS MORA

TÍTULO PRIMERO

Disposiciones Generales

ARTÍCULO 1

Las Políticas tienen por objeto establecer acciones generales y mecanismos para el cumplimiento de los principios, deberes, derechos y obligaciones en materia de datos personales, de conformidad con lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público. Asimismo, buscan divulgar las directrices y criterios generales relacionados con el procedimiento de atención a solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales en posesión del Instituto de Investigaciones Dr. José María Luis Mora.

ARTÍCULO 2

Además de las definiciones contenidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para efectos de las Políticas se entenderá por:

I. **Acuerdo de Confidencialidad:** documento cuyo objeto es que el personal interno y terceros distintos al personal del Instituto de Investigaciones Dr. José María Luis Mora mantengan la confidencialidad respecto a los datos que, por alguna razón, pudieran conocer;

II. **Activo:** es un recurso (ya sea material o físico, como documentos, servicios, prácticas, políticas, instalaciones; técnico como software o hardware, o humano, como personas) que tiene valor para la organización del Instituto de Investigaciones Dr. José María Luis Mora y necesita ser protegido de potenciales riesgos;

III. **Área o áreas competentes:** áreas administrativas a las que se confieren atribuciones específicas en el Capítulo II, Unidades

Administrativas, del Manual General de Organización del Instituto de Investigaciones Dr. José María Luis Mora, para realizar actividades que involucran el tratamiento de datos personales;

IV. **Bloqueo:** consiste en identificar y conservar datos personales que ya han cumplido la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación;

V. **Comité de Transparencia:** instancia a la que hacen referencia los artículos 83 y 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

VI. **Criterio:** pauta que obliga a tomar en cuenta todos los elementos disponibles de un caso para elegir de entre las posibles alternativas la mejor, con la finalidad de establecer los principios para la resolución de casos subsecuentes;

VII. **Derechos ARCO:** son los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, conforme a lo siguiente:

a) **Acceso:** derecho de la persona titular para acceder, por sí o a través de su representante, a sus datos personales que obren en posesión del Instituto de Investigaciones Dr. José María Luis Mora, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

b) **Rectificación:** derecho de la persona titular para solicitar, por sí o a través de su representante, la corrección de sus datos personales que obren en posesión del Instituto de Investigaciones Dr. José María Luis Mora, cuando éstos resulten inexactos, incompletos o estén desactualizados.

c) **Cancelación:** derecho de la persona titular para solicitar, por sí o a través de su representante, la supresión de sus datos de los archivos, registros, expedientes y sistemas del Instituto de Investigaciones Dr. José María Luis Mora, a fin de que los mismo ya no estén en su posesión y dejen de ser tratados por este último. En ocasiones, procederá primero su bloqueo y, posteriormente, la supresión en las bases de datos.

d) **Oposición:** derecho de la persona titular para solicitar, por sí o a través de su representante, al Instituto de Instituto de Investigaciones Dr. José María Luis Mora se abstenga de realizar el tratamiento a sus datos o a exigir que éste cese, cuando aun siendo lícito el tratamiento considere que, de persistir, éste le causaría un daño o perjuicio; o, cuando sus datos personales sean objeto de un tratamiento

automatizado y éste le produzca efectos jurídicos no deseados o afecte de alguna manera sus intereses, derechos o libertades conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

VIII. Destinatario: persona física o moral, distinta al encargado, a quien el área competente transfiere datos personales para que efectúe un tratamiento independiente al realizado por el Instituto de Investigaciones Dr. José María Luis Mora;

IX. Documento: los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico.

X. Encargado: la persona física o jurídica, pública o privada, ajena a la organización de este Instituto de Investigaciones Dr. José María Luis Mora, que trata datos personales a nombre y por cuenta de este instituto, pero sin decidir sobre su tratamiento debido a que éste lo realiza siguiendo sus instrucciones;

XI. Enlace en materia de datos personales: persona o personas designadas por las personas titulares de cada área competente ante la Unidad de Transparencia, con la finalidad de mantener un vínculo de comunicación permanente para las gestiones derivadas de las normas aplicables en la materia;

XII. INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

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

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

XV. Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público;

XVI. Módulo de Transparencia: lugar físico ubicado en la Sede Plaza del Instituto de Investigaciones Dr. José María Luis Mora donde se brinda atención a las personas al realizar solicitudes de forma presencial y, cuando proceda, para entregar los documentos que correspondan a la respuesta con apoyo en lo previsto en las Políticas y demás normas aplicables en materia de datos personales;

XVII. Personal: las servidoras y los servidores públicos o empleados definidos en la Ley Orgánica del Poder Judicial de la Federación, que laboran en el Instituto de Investigaciones Dr. José María Luis Mora;

XVIII. Políticas: Políticas internas para la gestión y el tratamiento de los datos personales en posesión del Instituto de Investigaciones Dr. José María Luis Mora;

XIX. Remisión: toda comunicación de datos personales realizada entre las áreas competentes del Instituto de Investigaciones Dr. José María Luis Mora y el encargado del tratamiento de datos personales, dentro o fuera del territorio mexicano;

XX. Sistema o sistemas de datos personales: archivo físico, electrónico o mixto que contenga datos personales recabados en el ejercicio de las funciones, facultades y atribuciones de las áreas competentes;

XXI. Terceros: cualquier individuo diverso al personal que, por motivos académicos, proyectos, prestación de servicios o alguna otra causa, conozca los datos personales en posesión del Instituto de Investigaciones Dr. José María Luis Mora;

XXII. Transferencia: toda comunicación de datos personales nacional o internacional realizada a persona distinta de la persona titular, las áreas competentes del Instituto de Investigaciones Dr. José María Luis Mora o del encargado;

XXIII. Titular: la persona física a quien corresponden los datos personales, y

XXIV. Unidad de Transparencia: instancia a la que hacen referencia los artículos 85 y 87 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

ARTÍCULO 3

Las Políticas serán aplicables a cualquier tratamiento de datos personales que obren en soportes físicos, electrónicos o mixtos, ya sean estos últimos manuales o automatizados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, en posesión del Instituto Mora.

ARTÍCULO 4

Las Políticas tienen las finalidades siguientes:

I. Constituir un marco normativo de referencia para la protección de datos personales en posesión de las áreas competentes que integran al Instituto Mora;

II. Garantizar la observancia de los principios, deberes, obligaciones y derechos previstos en la Ley General, los Lineamientos Generales y demás normas que resulten aplicables en la materia;

III. Establecer medidas que garanticen, la integridad, disponibilidad y confidencialidad de los datos personales en posesión del Instituto Mora;

IV. Promover, fomentar y difundir una cultura de protección de datos personales en el Instituto Mora, y

V. Establecer acciones para el ejercicio de los derechos ARCO.

ARTÍCULO 5

Cada área competente designará al personal que fungirá como enlace en materia de datos personales y que será la encargada de apoyar a la persona titular de esa área a cumplir con lo establecido en las Políticas. Para tales efectos, tendrá las siguientes funciones:

I. Ser el enlace de comunicación con la Unidad de Transparencia para coordinar las acciones encaminadas al cumplimiento de los principios y deberes contenidos en la Ley General, en los Lineamientos Generales y en estas Políticas;

II. Orientar al interior de su área de adscripción sobre las obligaciones a cumplir cuando se implemente o modifique un trámite o procedimiento que involucre el tratamiento de datos personales;

III. Coadyuvar con la Unidad de Transparencia en los temas concernientes a la capacitación del personal de su área de adscripción que participe en el tratamiento de datos personales;

IV. Actualizar los inventarios de datos personales y avisos de privacidad que, en el ámbito de su competencia, correspondan al área de su adscripción;

V. Gestionar al interior del área, la debida atención de solicitudes relativas al ejercicio de los derechos ARCO que le sean turnadas por la Unidad de Transparencia;

VI. Remitir a la Unidad de Transparencia las solicitudes de ejercicio de los derechos ARCO que sean presentadas ante su área de adscripción a fin de dar cumplimiento al procedimiento previsto en los Lineamientos Generales.

VII. Coordinar la implementación de las medidas de seguridad para el resguardo del o los sistemas de datos personales bajo su responsabilidad de manera que se evite su alteración, reproducción, sustracción, difusión, destrucción o acceso no autorizado, o en su caso, la pérdida;

VIII. Contar con una relación actualizada del personal que tenga acceso a las bases o los sistemas de datos personales en su área de adscripción;

IX. Realizar el registro de las modificaciones sustanciales al tratamiento de datos personales;

X. Llevar la bitácora en la que se documenten las vulneraciones a la seguridad de los datos personales, y

XI. Cualquier otra actividad que se encuentre establecida en el Programa de Datos Personales, el Programa Anual de Capacitación en Materia de Datos Personales y el Documento de Seguridad o sea necesaria para el cumplimiento de éstos, así como de las obligaciones previstas en la Ley General y en los Lineamientos Generales.

ARTÍCULO 6

La Unidad de Transparencia atenderá las solicitudes de asesoría realizadas por las áreas competentes sobre la aplicación de las Políticas, con excepción de aquellas en las que se requiera interpretar o fijar criterio, lo cual le corresponderá al Comité de Transparencia. Una vez establecido, la Unidad de Transparencia desahogará la asesoría o consulta realizada.

Asimismo, corresponde al Comité de Transparencia interpretar las Políticas, en su calidad de máxima autoridad en materia de protección de datos personales del Instituto Mora, acorde con lo dispuesto en la Ley General.

TÍTULO SEGUNDO

Principios y deberes previstos en la Ley General y los Lineamientos Generales

CAPÍTULO I

De los principios

ARTÍCULO 7

Las áreas competentes serán las responsables de decidir sobre el tratamiento de los datos personales que obran en su poder, con motivo del ejercicio de sus funciones; establecer las finalidades del tratamiento; definir qué actividades en concreto realizarán con ellos y su uso; asimismo, determinarán el tipo de datos personales que requieren, su forma de obtención, almacenamiento, divulgación y supresión, así como cualquier aspecto relacionado con su ciclo de vida.

Para ello, deberán cumplir con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, tal como se establece en la Ley General, los Lineamientos y estas Políticas.

ARTÍCULO 8

Las áreas competentes deberán identificar las normas internas del Instituto Mora que las faculta a realizar el tratamiento de datos personales. En ese sentido, solo podrán tratar los datos personales para aquello que esté legalmente permitido.

Para cumplir con el principio de licitud, deberán incluir en el aviso de privacidad integral el marco normativo que las faculta a tratar datos personales para cada una de las finalidades referidas en dicho aviso.

ARTÍCULO 9

Los datos personales deben ser tratados exclusivamente para cumplir con la finalidad o finalidades para los cuales fueron recabados.

Se cumple con el principio de finalidad cuando el tratamiento de los datos personales que realicen las áreas competentes esté justificado en propósitos concretos, lícitos, explícitos y legítimos.

De conformidad con lo dispuesto en los Lineamientos Generales, se entenderá que las finalidades son:

I. **Concretas:** cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular;

II. **Explícitas:** cuando se expresen y den a conocer de manera clara en el aviso de privacidad;

III. **Lícitas:** cuando el tratamiento de los datos personales sea acorde con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y

IV. **Legítimas:** cuando el tratamiento de los datos personales se cuente con el consentimiento de la persona titular, salvo que se actualice alguna de las causales de excepción previstas en la Ley General.

Corresponderá a las áreas competentes identificar las finalidades de cada tratamiento de datos personales que realicen el cual deberá estar acorde con sus atribuciones. Asimismo, verificarán que en los avisos de privacidad se informen todas las finalidades para las cuales se tratan los datos personales y que éstas sean descritas de manera clara.

ARTÍCULO 10

De acuerdo con lo establecido en la Ley General, las áreas competentes podrán utilizar datos personales para finalidades diferentes a las establecidas en el aviso de privacidad, siempre y cuando cuenten con las atribuciones necesarias y obtengan el consentimiento de la persona titular de los datos.

En estos casos, las áreas competentes deberán identificar las normativas que les confieren las atribuciones legales para utilizar los datos personales con esas finalidades adicionales. Asimismo, deberán solicitar el consentimiento de las personas titulares para dicho tratamiento.

ARTÍCULO 11

Las áreas competentes establecerán los procedimientos necesarios y verificarán que los datos personales no se obtengan con dolo, mala fe o negligencia; Asimismo, se cerciorarán de que el tratamiento que realizan no

da lugar a discriminación o trato injusto o arbitrario en contra de la persona titular.

Para cumplir con el principio de lealtad, los avisos de privacidad, integrales y simplificados, deberán reflejar la realidad del tratamiento que se efectúa a fin de evitar confusiones.

ARTÍCULO 12

Previo al tratamiento de los datos personales, en aquellos casos en que se requiera el consentimiento en términos de lo previsto en la Ley General, las áreas competentes lo deberán obtener de manera libre, específica e informada.

Para cumplir con el principio de consentimiento, las áreas competentes identificarán las finalidades para las cuales se requiere. Posteriormente, definirán el tipo de consentimiento que se necesita (tácito o expreso), según las categorías de datos personales a tratarse o las normas aplicables que regulen el tratamiento; debiendo especificarlo en el aviso de privacidad respectivo.

Cuando no se requiera recabar el consentimiento de la persona titular de los datos personales, las áreas competentes responsables del tratamiento de datos personales deberán dar cumplimiento a las demás obligaciones establecidas en la Ley General, los Lineamientos Generales y estas Políticas.

Por regla general, el consentimiento tácito será válido para llevar a cabo el tratamiento de datos personales, salvo aquellos supuestos en los cuales la Ley General o alguna disposición aplicable exija su obtención de forma expresa o, en su caso, por escrito.

En el caso del consentimiento expreso, es necesario que las áreas competentes lo recaben directamente en el aviso de privacidad o en un mecanismo o documento aparte, el cual será generado por el área competente. En estos supuestos sólo se podrán tratar los datos personales para la finalidad respecto de la cual se otorgó el consentimiento de la persona titular, salvo que el tratamiento a realizar se encuentre en alguna de las hipótesis siguientes:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley General, en ningún caso, podrán contravenirla;

II. Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o

X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Corresponderá a las áreas competentes mantener, bajo su resguardo, el documento en el cual se haya manifestado el consentimiento de la persona titular para el tratamiento de sus datos, cuando éste proceda, así como implementar medidas para garantizar la puesta a disposición del aviso de privacidad a la persona titular, en aquellos casos en los cuales sea válido el consentimiento tácito.

Cuando los datos personales sean proporcionados por una persona física o moral distinta a su titular o su representante, el área competente deberá implementar medidas compensatorias, en términos de lo dispuesto en la Ley General, los Criterios generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal y demás normas aplicables.

ARTÍCULO 13

Las áreas competentes, a través de sus titulares y sus enlaces en materia de datos, deberán adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad, para lo cual deberán atender lo siguiente:

I. Los datos personales son exactos cuando reflejan la realidad de la situación de la persona titular, es decir, son verdaderos o fieles;

II. Los datos personales están completos cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados;

III. Los datos personales son pertinentes cuando corresponden efectivamente a la persona titular y no a una homonimia;

IV. Los datos personales están actualizados cuando corresponden a la situación presente de la persona titular, y

V. Los datos personales son correctos cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por la persona titular y hasta que ésta no manifieste y acredite lo contrario.

Las áreas competentes implementarán medidas para que los datos personales se actualicen y, en su caso, corrijan o completen, en las distintas bases o sistemas de datos que estén a su cargo, cuando derivado de sus funciones adviertan la existencia de alguna inconsistencia generada durante su tratamiento. En aquellos casos que la modificación o modificaciones deriven del ejercicio del derecho de rectificación previsto en la Ley General, éstas se realizarán dentro del plazo establecido en dicha norma jurídica.

En los casos referidos en el párrafo anterior, las áreas competentes deberán documentar las actualizaciones que realicen.

ARTÍCULO 14

Para cumplir con el principio de proporcionalidad, las áreas competentes identificarán y recabarán solo aquellos datos personales que resulten adecuados, relevantes y necesarios para cada una de las finalidades de los tratamientos que realizan.

Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas a las áreas competentes.

Cuando una norma establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, las áreas competentes sólo deberán solicitar dichos datos.

ARTÍCULO 15

Las áreas competentes, para dar cumplimiento al principio de información y, con independencia de que no se requiera del consentimiento de la persona titular para el tratamiento de sus datos personales, contarán con un aviso de privacidad integral y uno simplificado, por cada proceso en los que se traten datos personales.

Excepcionalmente, cuando dos o más procesos de tratamiento de datos personales, atiendan a una misma finalidad o función, se podrá contar con un mismo aviso de privacidad, en sus dos modalidades, siempre y cuando sea posible expresar con precisión y claridad las finalidades del tratamiento de datos personales, de tal manera que no dé lugar a incertidumbre o ambigüedad a las personas titulares.

En aquellos casos que no se requiera el consentimiento de las personas titulares para el tratamiento de datos personales, las áreas competentes les informarán sobre la existencia y las características principales del tratamiento

al que serán sometidos sus datos personales poniendo a disposición de forma física o electrónica el aviso de privacidad respectivo.

ARTÍCULO 16

En aquellos casos que se requiera el consentimiento de las personas titulares, sea tácito o expreso, previo a la recolección de los datos personales, se les informará, a través de los avisos de privacidad, los alcances y condiciones generales del tratamiento al que serán sometidos sus datos, a fin de que pueda tomar decisiones sobre su uso, en términos de lo previsto en la Ley General.

ARTÍCULO 17

El aviso de privacidad, simplificado e integral, será elaborado por las áreas competentes que realizarán el tratamiento de datos personales. En su integración y elaboración preverán un diseño que facilite su entendimiento por parte de las personas titulares de los datos.

Una vez elaborados los avisos de privacidad, deberán remitirse mediante oficio a la Unidad de Transparencia a fin de que se les dé seguimiento de acuerdo con lo establecido en el Programa de Protección de Datos Personales.

ARTÍCULO 18

Las áreas competentes se asegurarán de que la información contenida en los avisos de privacidad se redacte con un lenguaje sencillo, claro y comprensible, considerando en todo momento, el perfil de la persona titular al cual va dirigido, por lo que se abstendrán de:

I. Usar frases inexactas, ambiguas o vagas;

II. Incluir textos que induzcan a las personas titulares a elegir una opción en específico;

III. Marcar previamente casillas, en caso de que éstas se incluyan, para que las personas titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que el titular ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte, y

IV. Remitir a textos o documentos que no estén disponibles para las personas titulares.

ARTÍCULO 19

Una vez que los avisos de privacidad, simplificado e integral, cuenten con la validación de la Unidad de Transparencia, deberá publicarlos en el sitio destinado para tales efectos en la página de internet del Instituto Mora, con independencia de la difusión que las áreas competentes realicen en los lugares que consideren necesarios.

Corresponde a las áreas competentes verificar que sus avisos de privacidad, simplificados e integrales, se encuentran actualizados y publicados en el portal de internet del Instituto Mora.

ARTÍCULO 20

Cuando se requiera generar un nuevo aviso de privacidad en cualquiera sus dos modalidades, integral y simplificado, el área competente lo notificará por oficio a la Unidad de Transparencia, quien lo asesorará respecto a las obligaciones y deberes vinculadas con el tratamiento que da origen al nuevo aviso.

Posterior a esa comunicación, el área competente contará con un plazo no mayor a cinco días hábiles para elaborarlo y remitirlo a la Unidad de Transparencia para la validación correspondiente.

ARTÍCULO 21

Si el tratamiento de los datos personales implica cambios sustanciales, las áreas competentes deberán elaborar nuevos avisos de privacidad, simplificado e integral, que sustituyan los ya existentes. Se entenderá por cambios sustanciales los siguientes:

I. Por disposición del Manual General de Organización del Instituto de Investigaciones Dr. José María Luis Mora, o si el proceso de tratamiento de datos personales se traslada a una nueva área o esta cambia su denominación;

II. Se requieran recabar datos sensibles diversos a los informados en el aviso de privacidad original, los cuales no se obtengan de manera directa de la persona titular y se requiera de su consentimiento para el tratamiento de éstos;

III. Cambien las finalidades señaladas en el aviso de privacidad original, o

IV. Se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar otras no previstas inicialmente y, el consentimiento de la persona titular sea necesario.

ARTÍCULO 22

Cuando se requiera modificar el alcance o los datos de determinado tratamiento realizado por alguna área competente, se deberá remitir la propuesta de modificación a los avisos de privacidad correspondientes a la Unidad de Transparencia para su validación, en un plazo no mayor a tres días hábiles, previos a la modificación del tratamiento en cuestión.

En los casos en que la modificación atienda a un tratamiento para el cual se prevea normativamente un plazo distinto para su implementación, el área competente se sujetará a dichos plazos.

ARTÍCULO 23

Para la elaboración o actualización de los avisos de privacidad, las áreas competentes, en todo momento, podrán solicitar orientación técnica y asesoría a la Unidad de Transparencia.

ARTÍCULO 24

Para dar cumplimiento al principio de responsabilidad se deberá atender lo siguiente:

I. Cada área competente preverá el presupuesto necesario para la instrumentación de programas y políticas de protección de datos personales, estableciendo, entre su personal, su observancia y exigibilidad;

II. La Unidad de Transparencia, elaborará y someterá a la aprobación del Comité de Transparencia, las Políticas, el Documento de Seguridad, el Programa de Protección de Datos Personales, el Programa Anual de Capacitación en Materia de Datos Personales y sus respectivas modificaciones, cuyos cumplimientos serán obligatorios para el personal del Instituto Mora. En el caso del Programa Anual de Capacitación en Materia de Datos Personales también le corresponderá su aplicación;

III. La Unidad de Transparencia, en el ámbito de sus atribuciones, recibirá y atenderá las dudas y/o quejas de las personas titulares de los datos personales conforme a lo dispuesto en las Políticas;

IV. La Unidad de Transparencia, en coordinación con la Subdirección de Tecnologías de la Información y Comunicaciones, orientará a las áreas competentes a fin de que garanticen que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otro recurso tecnológico o digital que implique el tratamiento de datos personales en posesión del Instituto Mora, cumplan con las obligaciones previstas en la Ley General, y

V. Las áreas competentes diseñarán, desarrollarán e implementarán sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otro recurso tecnológico o digital que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley General y las demás que resulten aplicables en la materia.

ARTÍCULO 25

El Programa Anual de Capacitación en Materia de Datos Personales que apruebe el Comité de Transparencia, de conformidad con lo que establecen la Ley General y en los Lineamientos Generales, deberá ser obligatorio para el personal del Instituto Mora, atendiendo a los plazos y procedimientos que al efecto se establezcan en dicho Programa.

ARTÍCULO 26

La persona particular podrá presentar sus dudas y/o quejas físicamente en el Módulo de Transparencia, por correo electrónico a la Unidad de Transparencia, mediante formato libre o utilizar el formato que, en su caso, se establezca para tal efecto, el cual se podrá consultar en el micrositio de Transparencia de la página de Internet del Instituto Mora.

Si las dudas y/o quejas son presentadas en un área distinta a la Unidad de Transparencia, aquélla tendrá la obligación de remitirla a ésta de inmediato. Una vez recibida las dudas y/o quejas, la Unidad de Transparencia entregará el acuse de recibo correspondiente.

En caso de que el personal del Instituto Mora atienda vía telefónica a una persona que pretenda presentar una queja en esta materia, deberá canalizar la llamada a la Unidad de Transparencia o, en su caso, proporcionarle el correo electrónico institucional correspondiente.

ARTÍCULO 27

Las dudas y/o quejas que se presenten se atenderán en un plazo no mayor a quince días hábiles contados a partir del día hábil siguiente al de la recepción.

ARTÍCULO 28

Para la presentación de las dudas y/o quejas no se podrán exigir mayores requisitos que la descripción clara y precisa de los hechos o asesoría que se desee recibir, señalando cualquier elemento o documento que facilite orientar el sentido de la queja o duda.

Si para atender las dudas y/o quejas, resulta indispensable identificar a la persona titular de los datos personales en posesión del Instituto Mora, previo a entregarle la respuesta, deberá acreditar su identidad o la identidad y personalidad de su representado, de acuerdo con las reglas que para tal efecto se establecen en los Lineamientos Generales.

ARTÍCULO 29

En caso de que la respuesta a la duda genere costos de reproducción y/o envío, la persona solicitante deberá cubrirlos.

Para tales efectos, la Unidad de Transparencia deberá notificar a la persona solicitante el número de cuenta en que se debe realizar el pago, así como el medio para enviar el comprobante de pago respectivo.

ARTÍCULO 30

Cuando la Unidad de Transparencia considere que las dudas y/o quejas no están vinculadas con sus facultades y/o atribuciones, o no corresponden a las normas aplicables a la protección de datos personales en posesión del Instituto Mora, deberá informar a la persona solicitante la notoria incompetencia, dentro de los tres días hábiles siguientes a su presentación.

ARTÍCULO 31

Las dudas, en general, serán atendidas directamente por la Unidad de Transparencia; sin embargo, en el caso de que se requiera información específica de algún área competente, le solicitará que se pronuncie conforme a derecho proceda.

Para tales efectos, la Unidad de Transparencia dispondrá de un plazo máximo de dos días hábiles contados a partir del día hábil siguiente a su recepción para analizar el escrito y, en su caso, turnarlo al área competente para su correspondiente desahogo. Por su parte, el área competente contará con un plazo no mayor a ocho días hábiles para remitir su respuesta a la Unidad de Transparencia.

ARTÍCULO 32

Las quejas que se reciban deberán ser sometidas, por la Unidad de Transparencia, a consideración del Comité de Transparencia para que determine el procedimiento a seguir.

ARTÍCULO 33

En caso de que la Unidad de Transparencia advierta que las dudas y/o quejas presentadas corresponden a un derecho de los previstos en la Ley General, registrará la solicitud en la Plataforma Nacional de Transparencia, máximo al día hábil siguiente de haberla recibido y procederá a su trámite en los términos previstos en la propia Ley General, lo que deberá hacerse del conocimiento de la persona titular, máximo dentro de los tres días hábiles siguientes a la presentación de la duda y/o queja.

ARTÍCULO 34

En aquellos casos en que el INAI requiera al Instituto Mora algún informe relacionado con el tratamiento de los datos personales, la Unidad de Transparencia, a más tardar al día hábil siguiente de recibir la notificación por parte de dicho órgano colegiado, turnará la petición al área competente con el objeto de recabar lo solicitado.

CAPÍTULO II

De los deberes

ARTÍCULO 35

Además de los principios señalados en el Capítulo anterior, las áreas competentes cumplirán con lo siguiente:

I. Deber de confidencialidad y

II. Deber de seguridad

ARTÍCULO 36

El personal del Instituto Mora está obligado a guardar la confidencialidad y secrecía respecto de los datos personales de los que tenga conocimiento en

ejercicio de sus atribuciones y funciones, con independencia de la fase del tratamiento en la que intervengan; obligación que subsistirá aun después de finalizar su relación laboral.

En caso de que infrinjan esta obligación, se harán acreedoras a las sanciones previstas en la Ley General y el Documento de Seguridad, con independencia de lo que al efecto disponga la Ley General de Responsabilidades Administrativas, la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y demás normas aplicables.

ARTÍCULO 37

En los contratos, convenios de colaboración o cualquier otro instrumento jurídico mediante los cuales las áreas competentes realicen transferencias o remisiones, se deberán incluir cláusulas de confidencialidad, a fin de que los responsables de los datos transferidos y encargados guarden secrecía de éstos durante y posterior a la vigencia del instrumento jurídico.

ARTÍCULO 38

Si por alguna circunstancia fuera necesario e indispensable que terceros tengan acceso a datos personales en posesión del Instituto Mora, corresponderá a la persona titular del área competente contar con el acuerdo de confidencialidad firmado por éstos.

Asimismo, deberán implementar los controles y medidas de seguridad necesarios para garantizar la secrecía de los datos personales de los que tengan conocimiento dichas personas.

ARTÍCULO 39

En los cursos, talleres, seminarios o similares del Programa Anual de Capacitación en Materia de Datos Personales se deberán incluir temas orientados a sensibilizar al personal sobre la importancia de la confidencialidad de los datos personales.

ARTÍCULO 40

Las áreas competentes, además de observar las medidas de seguridad de carácter administrativo, físico y técnico para la protección y tratamiento de los datos personales, previstas en la Ley General y los Lineamientos Generales, deberán atender las señaladas en el Documento de Seguridad a fin de evitar cualquier afectación a éstos y de la persona titular.

Asimismo, podrán implementar medidas de seguridad adicionales a las referidas en el párrafo anterior que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad. En este supuesto, deberán hacer del conocimiento de la Unidad de Transparencia la actualización.

ARTÍCULO 41

Para garantizar que los datos personales sean tratados de forma adecuada, las personas titulares de las áreas competentes, en apego a lo dispuesto en el documento de seguridad, deberán:

I. Contar con un inventario de los datos y de los sistemas de tratamiento;

II. Adoptar las medidas necesarias para la conservación de los sistemas de datos personales en soporte físico o tecnológico, de manera que se evite su alteración, reproducción, pérdida o acceso no autorizado;

III. Instrumentar, monitorear y revisar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar, a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución;

IV. Designar al personal que realizará el tratamiento de los datos personales, así como su conservación observando en todo momento las funciones y/o atribuciones del puesto, lo cual deberá ser informado a la Unidad de Transparencia para el registro correspondiente, de conformidad con el inventario que para el efecto se establezca en el Programa de Protección de Datos Personales;

V. Asignar un espacio seguro y adecuado para la operación de los sistemas de datos personales. Se entiende por espacio seguro y adecuado aquel que permita el oportuno manejo, operación, almacenamiento y conservación de los datos personales. Dicho lugar deberá contar con condiciones de iluminación y atender las medidas previstas en el Documento de Seguridad;

VI. Establecer medidas para controlar el acceso físico o ingreso a los espacios donde se encuentra el equipamiento que soporta la operación o que aloja los sistemas de datos personales;

VII. Adoptar las medidas necesarias para contar con el respaldo de los sistemas informáticos de conformidad con las Políticas de Seguridad de la Información y Objetivos;

VIII. Implementar procedimientos para el control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas que traten datos personales de conformidad con las Políticas de Seguridad de la Información y Objetivos, y

IX. Establecer medidas de seguridad para evitar la alteración, reproducción, sustracción, difusión o destrucción no autorizada de información de los sistemas de datos personales, o en su caso, la pérdida.

Para dar cumplimiento a lo establecido en las fracciones V a la IX de este artículo, las áreas competentes deberán solicitar asesoría a la Unidad de

Transparencia y Subdirección de Tecnologías de la Información y Comunicaciones, según corresponda.

ARTÍCULO 42

Para la elaboración y actualización del inventario de datos personales y de los sistemas de tratamiento a los que se refieren la Ley General y los Lineamientos Generales, las áreas competentes identificarán, dentro del flujo de sus actividades sustantivas vinculadas a los procesos institucionales a su cargo, los tratamientos que realizan, así como las bases, registros o sistemas en los cuales están contenidos los datos personales.

En la identificación de las bases, registros o sistemas considerarán tanto los medios de obtención de los datos personales, como los formatos de su almacenamiento, ya sean éstos en físicos, electrónicos, o ambos.

Las áreas competentes deberán verificar que los tratamientos de datos personales y su inventario se encuentren actualizados. En caso de ser necesario adicionar o actualizar algún tratamiento, deberán dar aviso a la Unidad de Transparencia, dentro del plazo de diez días contados a partir de que se hubiere detectado, para realizar las modificaciones respectivas.

ARTÍCULO 43

En relación con el deber de seguridad y para cumplir con el deber de evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar que se atiendan los objetivos propuestos y, en su caso, implementar mejoras de manera continua, las áreas competentes en coordinación con la Unidad de Transparencia monitorearán continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;

II. Las modificaciones a los activos;

III. Las nuevas amenazas que no hayan sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar las que estén expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

VII. Los incidentes y vulneraciones de seguridad ocurridas**.**

ARTÍCULO 44

Con el objeto de verificar el debido cumplimiento de las Políticas, las áreas competentes deberán establecer acciones de revisión y procedimientos internos para tal efecto.

Asimismo, el Comité de Transparencia, de conformidad con lo dispuesto en la Ley General, podrá ordenar a la Unidad de Transparencia, la ejecución de acciones específicas de revisión.

ARTÍCULO 45

La Unidad de Transparencia, en coordinación con las áreas competentes, podrá solicitar al INAI se le incluya en el programa de auditorías voluntarias de conformidad con lo previsto en el Programa de Protección de Datos Personales.

ARTÍCULO 46

Con el resultado de las auditorías y revisiones realizadas, o bien derivado de la petición de un área competente, previa autorización del Comité de Transparencia, la Unidad de Transparencia coordinará las acciones para adoptar las medidas preventivas y correctivas necesarias para mejorar los mecanismos, términos y procedimientos en la materia de que se trate.

El Comité de Transparencia establecerá un plazo límite para que se corrijan las inconformidades detectadas o, en su caso, que sea contemplado como parte del plan de trabajo contenido en el Documento de Seguridad.

El Comité de Transparencia, por conducto de la Unidad de Transparencia, documentará las medidas efectivamente realizadas para la mejora continua en la implementación de estas Políticas y las que sean sujetas al procedimiento de revisión y/o auditorías.

TÍTULO TERCERO

Obligaciones previstas en la Ley General y los Lineamientos Generales

CAPÍTULO I

De las transferencias y remisiones

ARTÍCULO 47

En toda transferencia o remisión que se realice, el área competente deberá comunicar al receptor de los datos personales, el aviso de privacidad integral correspondiente y documentará dicha comunicación.

ARTÍCULO 48

Toda transferencia de datos personales que se lleve a cabo está sujeta al consentimiento de la persona titular, salvo las excepciones siguientes:

I. Cuando la transferencia esté prevista en la Ley General u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;

II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el Instituto Mora y el titular;

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el Instituto Mora y un tercero;

VIII. Cuando se trate de los casos en los que el Instituto Mora no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, o

IX. Cuando la transferencia sea necesaria por razones de seguridad nacional.

Las áreas competentes, por medio del aviso de privacidad correspondiente informarán a la persona titular de los datos personales, las finalidades de la transferencia, así como su destinatario. En caso de ser una transferencia que requiera de consentimiento, se habilitarán los mecanismos para que la persona titular manifieste su voluntad.

ARTÍCULO 49

Las transferencias de datos personales que realicen las áreas competentes que no estén previstas en las excepciones establecidas en la Ley General, deberán ser formalizadas mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico de conformidad con lo previsto en la Ley General y los Lineamientos Generales.

El instrumento que formalice la transferencia en términos de este artículo deberá contener, al menos, lo siguiente:

I. Identificación de los datos personales, el sistema o los sistemas de datos personales motivo de la transferencia;

II. Finalidad de la transferencia;

III. Las medidas de seguridad que implementará el destinatario para evitar el uso indebido de los datos personales, el sistema o sistemas de datos personales;

IV. Plazo durante el cual conservará el destinatario los datos, sistema o sistemas transferidos, el cual podrá ser ampliado mediante aviso al Instituto Mora. Para tales efectos, se deberán indicar las razones o motivos por los cuales es necesaria la ampliación, y

V. Señalar si, una vez concluidos los propósitos de la transferencia, los datos personales serán destruidos por el destinatario o devueltos al Instituto Mora, al igual que cualquier soporte o documento en que conste algún dato personal objeto de la transmisión. Para el caso de que, concluidos los propósitos de la transferencia, se estipule su destrucción por parte del destinatario, se deberá establecer la forma en la que se efectuará dicha actuación, debiéndose levantar constancia de tales hechos ante la presencia del titular del área competente que los transfirió.

ARTÍCULO 50

Previo a que las áreas competentes realicen las transferencias nacionales o internacionales, deberán avisar a la Unidad de Transparencia, a efecto de que verifique el cumplimiento de lo dispuesto en el artículo anterior, así como lo previsto en la Ley General, los Lineamientos Generales y demás normas aplicables.

ARTÍCULO 51

Cuando la comunicación de datos personales se realice fuera del territorio nacional, previo a su transferencia, el área competente se asegurará que el destinatario se obligue a proteger los datos personales conforme a los principios, deberes y obligaciones similares o equiparables a los previstos en la Ley General y demás normas aplicables en la materia, así como a los términos previstos en el aviso de privacidad que le será comunicado.

En todo caso, el Instituto Mora podrá solicitar la opinión del INAI respecto de las transferencias internacionales que se planteen, en términos de lo dispuesto en los Lineamientos Generales.

ARTÍCULO 52

Las remisiones nacionales e internacionales de datos personales que se realicen entre el área competente y el encargado se sujetarán a lo previsto en la Ley General y en los Lineamientos Generales.

En las remisiones, el encargado tratará los datos personales a nombre y por cuenta del Instituto Mora dentro del ámbito de actuación de la prestación del servicio debidamente formalizado y sin ostentar poder alguno de decisión sobre el alcance y contenido del tratamiento, limitando sus actuaciones a los términos fijados por el Instituto Mora.

ARTÍCULO 53

Corresponderá a las áreas competentes tomar las medidas necesarias para que cualquier relación jurídica entre el Instituto Mora y aquellos que funjan como encargados se formalice mediante contratos o instrumentos jurídicos que garanticen la confidencialidad de los datos personales, así como el debido tratamiento de los datos personales, a través de la implementación de mecanismos que, en la medida de lo posible, limiten las remisiones al mínimo indispensable para la prestación del servicio de que se trate.

ARTÍCULO 54

El instrumento jurídico mediante el cual se formalice la relación jurídica entre el Instituto Mora, por conducto del área competente y el encargado deberá incluir al menos las siguientes obligaciones para éste:

I. Realizar el tratamiento de los datos personales de acuerdo con las instrucciones del Instituto Mora;

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Instituto Mora;

III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;

IV. Informar al Instituto Mora cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;

V. Guardar confidencialidad respecto de los datos personales tratados;

VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el Instituto Mora, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales;

VII. Abstenerse de transferir los datos personales salvo en el caso de que el Instituto Mora así lo determine, o por mandato expreso de la autoridad competente;

VIII. Permitir al INAI o al Instituto Mora, realizar verificaciones en el lugar donde se lleva a cabo el tratamiento de los datos personales;

IX. Colaborar con el INAI en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y los Lineamientos Generales, proporcionando la información y documentación que se estime necesaria para tal efecto, y

X. Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de las obligaciones señaladas en este artículo.

ARTÍCULO 55

La subcontratación de servicios que impliquen el tratamiento de los datos personales previamente remitidos por el Instituto Mora sólo podrá llevarse a cabo cuando en el instrumento jurídico suscrito entre éste y el encargado se contemple dicha situación, debiendo el encargado formalizar, a su vez, la relación jurídica con el subcontratado, a través de cualquier instrumento jurídico que permita acreditar su existencia, alcance y contenido, en términos de las disposiciones legales aplicables.

En el instrumento jurídico de subcontratación, además de prever las cláusulas establecidas en el artículo anterior, se establecerá que la persona física o moral subcontratada asumirá las mismas obligaciones establecidas para el encargado.

ARTÍCULO 56

Las áreas competentes podrán contratar o adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice las condiciones y cuente con los mecanismos establecidos en la Ley General. Corresponde a la Subdirección de Tecnologías de la Información y Comunicaciones cerciorarse de dicha circunstancia.

CAPÍTULO II

De las mejores prácticas y evaluaciones de impacto

ARTÍCULO 57

En el caso de que las áreas competentes pretendan desarrollar o adoptar esquemas de mejores prácticas, que busquen obtener la validación o reconocimiento del INAI de conformidad con la Ley General, deberán realizarlo por conducto de la Unidad de Transparencia al ser el enlace institucional en la materia.

Asimismo, para la elaboración de una evaluación de impacto se observarán las reglas que al efecto se establecen en los Lineamientos Generales y las que se emitan, en su caso, de manera adicional.

CAPÍTULO III

Del Programa de Protección de Datos Personales

ARTÍCULO 58

El Instituto Mora contará con un Programa de Protección de Datos Personales, aprobado por el Comité de Transparencia, cuyo objetivo es determinar las pautas generales bajo las cuales se llevarán a cabo las tareas institucionales orientadas a mantener la observancia en el cumplimiento de los principios y deberes, así como a garantizar el derecho a la protección de datos personales al interior de este sujeto obligado, atendiendo a lo previsto en la Ley General y los Lineamientos Generales.

ARTÍCULO 59

La Unidad de Transparencia elaborará la propuesta de ajustes o actualizaciones al Programa de Protección de Datos personales, la cual será sometida a consideración del Comité de Transparencia para su revisión y, en su caso, aprobación.

CAPÍTULO IV

Del Documento de seguridad

ARTÍCULO 60

El Documento de Seguridad forma parte de los mecanismos implementados para asegurar el cumplimiento al deber de seguridad, cuyo objeto es establecer, de manera general, las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales tratados.

ARTÍCULO 61

El Documento de Seguridad deberá contener como mínimo, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

VII. El programa general de capacitación.

ARTÍCULO 62

En las actualizaciones que se realicen al Documento de Seguridad deberán participar todas las áreas competentes, a través de sus enlaces en materia de datos personales, quienes en todo momento observarán los principios y deberes a que se refieren la Ley General, los Lineamientos Generales y demás disposiciones legales aplicables.

Para la formulación de propuestas de actualización del Documento de Seguridad, la Unidad de Transparencia elaborará formatos, cuestionarios o cualquier otro instrumento de apoyo, que resulte útil para el cumplimiento de estas Políticas y demás normas aplicables en la materia.

Acorde con lo dispuesto en la Ley General, el Documento de Seguridad se actualizará en los supuestos siguientes:

I. Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo;

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con que se cuente;

III. Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida, y

IV. Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

ARTÍCULO 63

Cuando alguna de las áreas competentes se encuentre en alguno de los supuestos referidos, por conducto de su enlace en materia de datos personales, remitirá por escrito su propuesta de actualización a la Unidad de Transparencia para su debida revisión, análisis y, en su caso, someterá a consideración del Comité de Transparencia las actualizaciones conducentes, quien resolverá al respecto.

Asimismo, podrán solicitar orientación técnica y asesoría a la Unidad de Transparencia, para la integración o cualquier acto relacionado con los alcances del Documento de Seguridad.

ARTÍCULO 64

La persona titular del área competente podrá solicitar en cualquier momento a su enlace en materia de datos personales, los informes que se requieran sobre las acciones contenidas en el Documento de Seguridad.

ARTÍCULO 65

Las áreas competentes llevarán una bitácora, en la cual anotarán cualquier modificación sustancial al tratamiento de datos personales que detentan, debiéndola notificar a la Unidad de Transparencia, dentro de los tres días hábiles siguientes a aquél en que haya ocurrido, a efecto de que esta última analice si dicho cambio conlleva un riesgo que haga necesario actualizar el Documento de Seguridad.

ARTÍCULO 66

En la bitácora donde las áreas competentes anoten cualquier modificación sustancial al tratamiento de datos personales también se registrará cualquier amenaza o vulneración a la seguridad de los datos personales de conformidad con lo dispuesto en el Programa de Protección de Datos Personales. De igual manera se anotarán las acciones realizadas para su mitigación.

En estos casos, se deberá describir: la fecha en que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva, a efecto de cumplir con lo dispuesto en la Ley General.

ARTÍCULO 67

En caso de presentarse alguna vulneración de seguridad que, de forma significativa afecte los derechos patrimoniales o morales de la persona titular, las áreas competentes lo deberán notificar a la Unidad de Transparencia, dentro en un plazo máximo de doce horas de ocurrido el evento, para que ésta, a su vez, lleve a cabo el proceso previsto en la Ley General y los Lineamientos Generales en estos casos.

ARTÍCULO 68

En términos de lo previsto en la Ley General, se consideran vulneraciones a la seguridad de los datos, las siguientes:

I. La 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.

ARTÍCULO 69

Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de las personas titulares, las áreas competentes involucradas, deberán generar un informe detallado que contenga al menos lo siguiente:

I. La naturaleza del incidente;

II. Los datos personales comprometidos;

III. Las recomendaciones a la persona titular acerca de las medidas que puede adoptar para proteger sus intereses;

IV. Las acciones correctivas implementadas para mitigar la vulneración;

V. Los datos de contacto del enlace responsable o personal al cual puede acudir la persona titular para obtener más información al respecto, y

VI. Los datos de contacto con que cuente el área competente del titular de los datos vulnerados.

El referido informe será remitido a la Unidad de Transparencia en un plazo no mayor a dos días hábiles posteriores a que se haya confirmado la vulneración, para que ésta lo haga del conocimiento de las personas titulares de los datos involucrados, a través del medio de contacto proporcionado por el área competente, y del Comité de Transparencia.

Adicionalmente, las áreas competentes deberán incluir en el informe a notificarse al INAI por parte de la Unidad de Transparencia lo dispuesto en los Lineamientos Generales.

ARTÍCULO 70

Conforme a lo previsto en los Lineamientos Generales, se entenderá que los derechos patrimoniales de la persona titular se afectan cuando la vulneración esté relacionada con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

Para el caso de los derechos morales, se entenderán aquellos relacionados, de manera enunciativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico o menoscabe ilegalmente la libertad o la integridad, física o psíquica de la persona titular de los datos.

ARTÍCULO 71

En aquellos casos en los cuales no sea posible notificar directamente a las personas titulares de los datos el informe referido en estas Políticas o ello implique esfuerzos desproporcionados, las áreas competentes instrumentarán medidas compensatorias de comunicación para tal efecto, como son: página de Internet institucional del Instituto Mora, carteles o cápsulas informativas u otro similar.

ARTÍCULO 72

El Comité de Transparencia podrá determinar la implementación de acciones adicionales a las realizadas por las áreas competentes para evitar futuras vulneraciones y reforzar las medidas de seguridad aplicables.

Para tal efecto, el Comité de Transparencia podrá auxiliarse de la asesoría, orientación o apoyo de otras áreas competentes, proponer la suscripción de convenios de colaboración o solicitar la contratación de especialistas en la materia, siempre y cuando exista la suficiencia presupuestal para ello.

CAPÍTULO V

Del proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad

ARTÍCULO 73

Las áreas competentes deberán monitorear periódicamente los mecanismos y medidas de seguridad que tienen implementados para verificar su eficacia; asimismo, revisarán que se encuentren debidamente reportados en el Documento de Seguridad vigente.

Cuando, derivado del monitoreo realizado se advierta la necesidad de actualizar los mecanismos y medidas de seguridad, el área deberá realizar un análisis de riesgo respecto del tratamiento que requiera ajustar las medidas de seguridad, a efecto de poder realizar el análisis de brecha correspondiente.

Una vez que se cuenta con el análisis de brecha, el área competente elaborará una propuesta respecto a las medidas y mecanismos a actualizar; podrá solicitar la opinión de la Unidad de Transparencia y

Subdirección de Tecnologías de la Información y Comunicaciones, de acuerdo con la propuesta realizada, respecto de su idoneidad para reducir la brecha planteada.

En todos los casos, deberán remitir la propuesta a la Unidad de Transparencia para verificar que no se ponga en riesgo algún otro activo; y una vez implementada la medida deberá dar aviso, mediante oficio, a la Unidad de Transparencia para que lo incorpore en el expediente respectivo y, en su momento, se incorpore al Documento de Seguridad del Instituto Mora.

CAPÍTULO VI

Del Programa de capacitación

ARTÍCULO 74

El Programa Anual de Capacitación en materia de protección de datos personales es uno de los mecanismos a través de los cuales se cumple con el principio de responsabilidad, el cual considerará los niveles de capacitación atendiendo a los roles y responsabilidades de quienes tratan los datos personales y conforme a lo previsto en la Ley General de Datos y en los Lineamientos Generales.

ARTÍCULO 75

El Comité de Transparencia será el órgano encargado de aprobar el Programa Anual de Capacitación, con base en la propuesta que sea presentada por la Unidad de Transparencia, en la cual se consideren las necesidades de capacitación de las áreas competentes y la oferta de capacitación del Instituto.

CAPÍTULO VII

De la portabilidad

ARTÍCULO 76

Para cumplir con la prerrogativa de portabilidad de los datos personales se deberán realizar las acciones y procedimientos necesarios previstos en la Ley General, en los Lineamientos Generales y en los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

CAPÍTULO VIII

De los roles y responsabilidades específicas de los involucrados en el tratamiento de datos personales

ARTÍCULO 77

Para efectos de cumplir con lo dispuesto en la Ley General respecto a los roles y responsabilidades específicas de los involucrados internos de las áreas competentes, cada inventario de datos personales sometidos a tratamiento contemplará un apartado específico para que, de manera precisa, se indiquen las servidoras públicas y los servidores públicos que realizan el tratamiento, su

área de adscripción y cuál es el tratamiento específico que realizan, conforme a lo dispuesto en el Documento de Seguridad.

De acuerdo con su nivel jerárquico, dichas personas, tendrán las siguientes obligaciones:

I. **Mandos superiores:** les corresponderá supervisar el tratamiento realizado, así como acercarse con las áreas especializadas en caso de considerar que las medidas de seguridad implementadas sean las necesarias para garantizar la integridad de los datos personales; asimismo, llevarán el control de alta y baja de las servidoras y los servidores públicos que pueden tener acceso a los datos personales en tratamiento;

II. **Mandos medios:** Coadyuvar en la actualización de registros de las servidoras y los servidores públicos que realizan tratamiento; así como solicitar la cancelación de los permisos respectivos cuando una persona deje de laborar para el Instituto Mora, y

III. **Nivel Operativo:** Conocer las medidas de seguridad que debe implementar al tratar los datos personales y verificar qué medidas tomar en caso de vulnerar los datos personales.

ARTÍCULO 78

Quienes realicen el tratamiento de los datos derivado de una remisión o transferencia deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como las obligaciones establecidas en estas Políticas.

ARTÍCULO 79

En caso de que la persona titular del área competente lo considere necesario, podrá anexar al inventario del tratamiento, un documento en el que realice las aclaraciones a que haya lugar respecto de las obligaciones de cada persona servidora pública.

CAPÍTULO IX

Del ciclo de vida de los datos personales

ARTÍCULO 80

Los datos personales se pueden obtener de tres formas:

I. **De forma personal:** cuando la persona titular proporciona los datos personales físicamente a las áreas responsables;

II. **De manera directa:** cuando la persona titular proporciona los datos personales por algún medio que permite su entrega directa a las áreas competentes, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, Internet o vía electrónica, entre otros, y

III. **De manera indirecta:** cuando las áreas competentes obtienen los datos personales sin que la persona titular se los haya proporcionado de forma personal o directa, como podría ser a través de transferencias o fuentes de acceso público.

Se considerarán como fuentes de acceso público aquellas que se encuentren previstas en la Ley General.

ARTÍCULO 81

En la obtención de los datos personales sujetos a tratamiento, las áreas competentes observarán las reglas establecidas en estas Políticas para los principios de licitud, lealtad, información, consentimiento y proporcionalidad.

ARTÍCULO 82

Las áreas competentes, en atención a sus normas aplicables, determinarán los medios de almacenamiento en los cuales se guardarán los datos personales que tratan, los cuales pueden ser físicos, electrónicos o mixtos.

ARTÍCULO 83

El uso de los datos personales se sujetará a las reglas establecidas en estas Políticas para los principios de finalidad y calidad; así como a las normas y procedimientos establecidos al interior del Instituto Mora.

ARTÍCULO 84

En eliminación de los datos personales, las áreas competentes deberán considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:

I. **Irreversibilidad:** que el proceso utilizado no permita recuperar los datos personales;

II. **Seguridad y confidencialidad:** que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y en los Lineamientos Generales, y

III. **Favorable al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

ARTÍCULO 85

Las áreas competentes establecerán el periodo durante el cual conservarán los datos personales, atendiendo a la finalidad para la cual fueron obtenidos originalmente.

Para ello, las áreas competentes observarán, las normas aplicables en la materia, así como las relativas a la gestión documental y administración de archivos que resulte aplicable.

Agotado el periodo de conservación, los datos personales, previo bloqueo, en su caso, deberán ser suprimidos de las bases o registros, observando los parámetros generales que para tal efecto se establezcan en el Programa de Protección de Datos Personales y las normas en materia archivística, en cumplimiento a lo dispuesto en los Lineamientos Generales.

Asimismo, las áreas competentes que tengan sistemas de datos personales deberán documentar las medidas implementadas para su conservación y, en su caso, bloqueo y supresión de los datos personales, actividades en las que deberán incluir los plazos de conservación.

ARTÍCULO 86

Las áreas competentes deberán establecer métodos de organización interna que les permitan verificar que no realizan tratamiento excesivo de datos personales.

Hay tratamiento excesivo cuando se solicite a las personas titulares mayores datos de los indispensables para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas a las áreas competentes por las normas aplicables.

TÍTULO CUARTO

Derechos ARCO

CAPÍTULO I

Del procedimiento para el ejercicio de los Derechos ARCO

ARTÍCULO 87

Las áreas competentes están obligadas en todo momento a garantizar las condiciones necesarias para el adecuado tratamiento de los datos personales, así como la debida administración y custodia de los datos personales que se encuentren bajo su resguardo, con el objeto de maximizar el ejercicio de los derechos ARCO.

Para registrar, tramitar y dar respuesta a las solicitudes de derechos ARCO, la Unidad de Transparencia y las áreas competentes deberán atender lo señalado en la Ley General y los Lineamientos Generales.

ARTÍCULO 88

La presentación de solicitudes de derechos ARCO podrá realizarse a través de los medios de recepción siguientes:

I. Unidad de Transparencia del Instituto Mora;

II. Correo electrónico de la Unidad de Transparencia, y

III. Plataforma Nacional de Transparencia.

ARTÍCULO 89

En todo momento la persona titular o su representante, pueden ejercer ante la Unidad de Transparencia, los derechos ARCO de los datos personales que le conciernen, de conformidad con lo establecido en las Políticas, la Ley General, en los Lineamientos Generales y demás normas aplicables.

ARTÍCULO 90

El ejercicio de los derechos ARCO por persona distinta a la persona titular o a su representante, incluyendo los datos de personas fallecidas, será posible, en los supuestos previstos en la Ley General y en los Lineamientos Generales.

ARTÍCULO 91

Para el ejercicio de los derechos ARCO, es necesario que la persona titular acredite su identidad y, de ser el caso, la identidad y personalidad con la que actúe su representante en cualquiera de los siguientes momentos:

I. Al presentar la solicitud, en términos de lo dispuesto en la Ley General y los Lineamientos Generales;

II. Cuando se le notifique la respuesta sobre el ejercicio de los derechos ARCO, de acuerdo con lo que al efecto señalan la Ley General y los Lineamientos Generales, o

III. Al momento de entregar la constancia que acredite el ejercicio efectivo de los derechos ARCO, de conformidad con la Ley General y los Lineamientos Generales.

ARTÍCULO 92

La persona titular tiene derecho a solicitar la rectificación o corrección de sus datos personales que obren en poder del Instituto Mora, cuando éstos resulten ser inexactos, incompletos o estén desactualizados, de conformidad con Ley General y las demás normas aplicables.

La rectificación puede hacerse en cumplimiento al principio de calidad, siempre y cuando el área competente responsable del tratamiento tenga en su posesión los documentos inexactos, incompletos o desactualizados.

Para ejercer este derecho, la persona titular o su representante deberán contar con los documentos necesarios en original, expedidos por autoridad competente y que cumplan con todos los requisitos de validez que dispongan las leyes respecto del acto del que se trate, los cuales serán presentados como medio de prueba ante el Instituto Mora para determinar si es procedente su petición.

ARTÍCULO 93

La cancelación puede dar lugar al bloqueo de los datos en el que el área competente los conservará precautoriamente para efectos de responsabilidades, hasta el plazo de prescripción legal o contractual de éstas.

Durante dicho periodo, los datos personales no pueden ser objeto de tratamiento, y transcurrido éste, se procederá a su supresión en la base, sistema o sistemas de datos personales que corresponda.

ARTÍCULO 94

Cuando sea procedente el ejercicio de los derechos de rectificación y/o cancelación, el área competente adoptará todas aquellas medidas para que los datos personales sean corregidos o suprimidos, según corresponda. En caso de haberse realizado transferencias o remisiones y resulte procedente la rectificación o cancelación, se informará la situación a las personas destinatarias o personas encargadas para que procedan a la corrección o supresión, según sea el caso.

ARTÍCULO 95

La persona titular podrá oponerse, previa petición, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos personales que le conciernen sean objeto de tratamiento por las funciones y/o atribuciones propias del ejercicio del poder público conferido al Instituto Mora, salvo que exista mandamiento legal en contrario por lo que la excepción deberá estar fundada y motivada.

ARTÍCULO 96

Una vez presentada la solicitud de derechos ARCO, la Unidad de Transparencia, a más tardar a los dos días hábiles siguientes de su recepción, la turnará al área competente que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales.

ARTÍCULO 97

Las áreas competentes llevarán a cabo las acciones pertinentes para garantizar el efectivo ejercicio de los derechos ARCO de las personas titulares, acorde con los principios, obligaciones y deberes en materia de protección de datos personales.

ARTÍCULO 98

Si la solicitud de derechos ARCO no cumple con los requisitos previstos en la Ley General, el área competente a la que se hubiera turnado la solicitud, formulará una prevención dentro de un plazo que no podrá exceder de tres días hábiles contados a partir de la presentación de la solicitud, para que la Unidad de Transparencia notifique a la persona solicitante y ésta dentro del plazo de diez días hábiles contados a partir del día hábil siguiente al de la notificación, aporte los elementos necesarios para darle trámite.

ARTÍCULO 99

Si la solicitud de derechos ARCO es procedente, el área competente deberá notificarlo a la Unidad de Transparencia, dentro de los ocho días hábiles siguientes en que se le haya turnado la solicitud.

ARTÍCULO 100

Si el área competente considera que la solicitud de derechos ARCO es improcedente, dentro de los ocho días hábiles siguientes a aquél en que haya recibido la solicitud, deberá remitir al Comité de Transparencia, por conducto de la Unidad de Transparencia, un oficio a través del cual funde y motive la improcedencia. En todo caso, el Comité de Transparencia emitirá una resolución fundada y motivada, en la que confirme, modifique o revoque la improcedencia de la solicitud de derechos ARCO.

ARTÍCULO 101

En caso de que el área competente requiera de un plazo mayor a los ocho días hábiles referidos en los artículos anteriores, deberá hacerlo del conocimiento de la Unidad de Transparencia, indicando la fecha en la que dará respuesta.

Si la fecha de respuesta señalada por el área competente en el párrafo anterior supera los veinte días hábiles que tiene el Instituto Mora para dar respuesta, se deberá enviar un oficio, solicitando a la Unidad de Transparencia la aprobación de la ampliación del plazo de respuesta por parte del Comité de Transparencia, fundando y motivando las razones por las cuales el área se encuentra impedida materialmente para dar atención a la solicitud en el período ordinario.

La ampliación que en su caso se apruebe será únicamente y de forma excepcional por diez días hábiles adicionales, siempre que se justifique plenamente alguna necesidad que responda a causas extraordinarias, verificadas y verificables y sin que por ello puedan entenderse las cargas cotidianas de trabajo.

En caso de que la ampliación no sea aprobada, el área competente deberá proporcionar la respuesta conducente en un plazo no mayor de dos días hábiles contados a partir de que tenga conocimiento de dicha situación, para que la Unidad de Transparencia pueda otorgar la respuesta a la persona solicitante dentro del plazo legal.

ARTÍCULO 102

La presentación de la solicitud de derechos ARCO es gratuita. No obstante, si ésta implica una respuesta que conlleve la reproducción en copia simple o certificada, se aplicará una cuota correspondiente a los costos de reproducción y, en su caso, del envío, salvo las excepciones previstas en las leyes en la materia.

Si la persona titular proporciona el medio electrónico o el mecanismo necesario para reproducir la respuesta a la solicitud de derechos ARCO, la misma se entregará sin costo a éste.

Los costos de envío o reproducción deberán ser cubiertos por el solicitante de forma previa a la entrega de la respuesta, por lo que la Unidad de Transparencia deberá notificar la forma y modo en la que la persona solicitante deberá acreditar el pago respectivo.

La Unidad de Transparencia deberá consultar los costos de reproducción que se encuentren vigentes, y autorizados por el Comité Transparencia o, en su caso, solicitar a la Dirección de administración y Finanzas, que informe el costo de envío, el cual será determinado en cada caso, previa cotización expedida por una compañía de mensajería.

Sin perjuicio de lo anterior, la respuesta a la solicitud de derechos ARCO deberá ser entregada sin costo, cuando implique la entrega de no más de veinte fojas simples o certificadas. No obstante, si la respuesta supera este número de fojas, la persona solicitante cubrirá el costo de las fojas excedentes.

ARTÍCULO 103

Cuando algún área competente se vea impedida legalmente para atender este procedimiento, deberá implementar las acciones necesarias que le permitan garantizar la protección de datos personales maximizando en lo posible el ejercicio de los derechos ARCO.

ARTÍCULO 104

Para dar cumplimiento a lo dispuesto en la Ley General, la Unidad de Transparencia deberá mantener en evaluación continua los procedimientos internos para la gestión de las solicitudes de ejercicio de derechos ARCO, entre otros mecanismos, mediante la aplicación de indicadores de gestión con la periodicidad que, para este efecto, determine aplicable.

CAPÍTULO II

Del Recurso de Revisión

ARTÍCULO 105

Cuando el INAI notifique la admisión del recurso de revisión al Instituto Mora, se realizará el siguiente proceso:

I. La Unidad de Transparencia deberá turnar el recurso de revisión y el acuerdo de admisión al área competente en un plazo de un día hábil;

II. El área competente deberá remitir mediante oficio sus alegatos en un plazo no mayor de tres días hábiles contados a partir de la recepción de la notificación del recurso, y

III. La Unidad de Transparencia enviará los alegatos al INAI dentro del plazo de siete días hábiles establecido para ello.

Los plazos referidos en las fracciones anteriores estarán sujetos al plazo que el INAI establezca en el acuerdo de admisión para remitir los alegatos.

Las áreas competentes deberán coadyuvar en todo momento con la Unidad de Transparencia, a efecto de desahogar en tiempo y forma los requerimientos o audiencias que en su caso llegue a solicitar el INAI. La Unidad de Transparencia podrá brindar el acompañamiento necesario al área competente, cuando resulte procedente.

ARTÍCULO 106

Una vez notificada la resolución del recurso de revisión a la Unidad de Transparencia se realizará el siguiente procedimiento:

I. La Unidad de Transparencia deberá notificar al área competente la resolución del recurso de revisión, a más tardar el día hábil siguiente de su notificación por parte del INAI;

II. En caso de que la resolución del INAI conlleve alguna instrucción, la Unidad de Transparencia notificará las acciones conducentes ordenadas por el INAI a las áreas competentes, las cuales deberán atenderlas en el plazo que le señale la Unidad de Transparencia, a efecto de estar en aptitud de cumplimentar la resolución del Órgano Garante en el plazo establecido para dichos efectos;

III. En caso de que el INAI requiera mayores acciones para dar por cumplida la resolución, la Unidad de Transparencia deberá notificar a las áreas competentes las acciones requeridas, señalándole el plazo para dar cumplimiento;

IV. En caso de que se requiera que el Comité de Transparencia ejerza sus facultades de conformidad con la Ley General, la Unidad de Transparencia realizará las gestiones necesarias para que los integrantes del comité sesionen dentro del plazo otorgado para dar cumplimiento a la resolución, y

V. La Unidad de Transparencia deberá informar al INAI sobre las acciones llevadas a cabo para dar cumplimiento a la resolución en el plazo establecido por el INAI.

TÍTULO QUINTO

De las sanciones

ARTÍCULO 107

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en la Ley General, estas Políticas y demás normas exigibles al interior del Instituto Mora, por conducto de la Unidad de Transparencia, realizará un exhorto al área competente 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, el Comité de Transparencia tomará las medidas necesarias para que las servidoras y los servidores públicos que están a cargo del tratamiento de datos personales conozcan las causas de sanción por incumplimiento de las obligaciones establecidas en la Ley General.

ARTÍCULO 108

En la Ley General y Programa de Protección de Datos Personales se establecen las causas de sanción por incumplimiento a las obligaciones en materia de datos personales.

TRANSITORIOS

PRIMERO. Estas Políticas entrarán en vigor al día hábil siguiente de su aprobación.

SEGUNDO. Para su mayor difusión, publíquense en el portal de internet e intranet del Instituto de Investigaciones Dr. José María Luis Mora.