Políticas Internas para el Tratamiento, Gestión y Protección de los Datos Personales en el Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD)

INDICE **PÁGINA**

1. OBJETIVO

La presente política busca establecer los deberes, reglas, principios, tratamiento y gestión de datos personales que deben observar las diferentes áreas dentro del Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD), que, en el ejercicio de sus funciones y atribuciones conferidas, involucren en sus procesos el manejo de Datos Personales.

2. ALCANCE

La presente política es de observancia general para todos los servidores públicos adscritos al CIAD cuya labor incluya la administración y tratamiento de datos personales.
A raíz de lo anterior, el Centro de Investigación en Alimentación y Desarrollo, A.C. (CIAD), se compromete con cumplir y obedecer conforme a los principios y obligaciones establecidos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, con el objetivo de dar cumplimiento a dicha normatividad. Quedan excluidos aquellos Datos Personales que en las labores de cumplimiento de las obligaciones de transparencia no requieran consentimiento alguno de la persona titular, en base a lo mencionado en los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

3. INTRODUCCIÓN

Conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su artículo 3, fracción IX, menciona que los Datos Personales son “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”, hablamos pues de la privacidad y datos relativos a la vida privada de una persona, que, de ser mal usados, pudiesen llegar a generar un daño al titular de dichos datos, a raíz de ello parte la importancia del derecho a la Protección de Datos Personales.

La Constitución Política de los Estados Unidos Mexicanos menciona en su artículo 6; que todas las personas tienen derecho al libre acceso a la información pública, a sus Datos Personales y a la rectificación de los mismos, dicho derecho deberá ser protegido por el Estado, aunado a ello, el artículo 16, párrafo segundo, reitera la protección a los datos personales, del mismo modo, deberá salvaguardarse el derecho al acceso, rectificación, cancelación y oposición de los Datos Personales de las personas.

La presente política está elaborada con fundamento en lo establecido por el artículo 30, fracciones I y II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 47 de los Lineamientos para la Protección de Datos Personales, los cuales establecen que los responsables deberán elaborar e implementar políticas y programas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de Datos Personales a efecto de proteger éstos de manera sistemática y continúa.

4. FUNDAMENTO LEGAL

a) Constitución Política de los Estados Unidos Mexicanos, artículo 6, Base A y segundo párrafo del artículo 16.
b) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 30, fracción II, 33, fracción I, 83 y 84 fracción I.

5. GLOSARIO

Con el fin de hacer efectiva la presente política de Datos Personales, se utilizará los siguientes términos:

- **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 de estos.
- **CIAD:** Centro de Investigación en Alimentación y Desarrollo, A.C.
- **COMITÉ DE TRANSPARENCIA:** Comité de Transparencia del Centro de Investigación en Alimentación y Desarrollo, máxima autoridad en materia de datos personales, encargada de la administración, supervisión, y aseguramiento necesario para garantizar el derecho a la protección de datos personales acorde al artículo 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- **CONSENTIMIENTO:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de estos.
- **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, pueden incluir información relacionada con; el nombre, sexo, el estado civil, la nacionalidad, lugar y fecha de nacimiento, idioma o lengua y ocupación.

- **DATOS PERSONALES SENSIBLES:** Aquella información concerniente a los aspectos más íntimos de las personas, cuyo mal uso no autorizado puede generar discriminación o provocar situaciones de grave riesgo, pueden incluir información relacionada con; el origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
- **DERECHOS ARCO:** Derechos de Acceso, Rectificación, Cancelación y Oposición, todos relacionados con el manejo de datos personales.
- **INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- **LFTAIP:** Ley Federal de Transparencia y Acceso a la Información Pública.
- **LGPDPPSO:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **LGTAIP:** Ley General de Transparencia y Acceso a la Información Pública.
- **LINEAMIENTOS GENERALES:** Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- **TITULAR:** La persona física a quien corresponden los Datos Personales, y quien es considerado como sujeto de protección del Derecho a la protección de los Datos Personales.
- **TRANSFERENCIA:** La Transferencia es toda comunicación de Datos Personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.
- **UNIDAD DE TRANSPARENCIA:** Unidad encargada de la recepción y trámite de solicitudes de información, recabar la información interna requerida en atención a las solicitudes, promover y fomentar la transparencia al interior del sujeto obligado acorde al artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.
- **VULNERACIÓN:** Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

6. PRINCIPIOS

Acorde al artículo 16 de la LGPDPPSO y 8 de los Lineamientos Generales, todos los servidores públicos que integren el CIAD deben respetar y aplicar los siguientes principios durante el manejo de Datos Personales:

I. Licitud;

II. Finalidad;

III. Lealtad;

IV. Consentimiento:

V. Calidad;

VI. Proporcionalidad;

VII. Información, y

VIII. Responsabilidad.

A. PRINCIPIO DE LICITUD

El responsable debe tratar a los datos personales en su posesión sujetándose a las atribuciones y facultades que la normatividad aplicable le confiera, así mismo, respetando los derechos y libertades de los titulares.

B. PRINCIPIO DE FINALIDAD

Los Datos Personales deben ser usados por el titular conforme a las atribuciones conferidas dentro de los procesos de gestión señalados en el aviso de privacidad del CIAD, mismos que deben respetar lo señalado por la normatividad aplicable.

C. PRINCIPIO DE LEALTAD

No se deberá recabar Datos Personales a través de medios engañosos o fraudulentos, se revisará que los procedimientos y formatos utilizados para la recepción de información no se hagan de forma dolosa, de mala fe o con negligencia, buscando siempre el respeto a la privacidad de la persona titular de los Datos Personales.

D. PRINCIPIO DE CONSENTIMIENTO

Toda área que realice gestiones de Datos Personales deberá contar con el consentimiento del titular para que sus datos sean tratados, acorde a la finalidad para los que sean recabados.

E. PRINCIPIO DE CALIDAD

Acorde al propósito con el que tratarán los Datos Personales, estos deberán ser exactos, pertinentes, actualizados, completos y correctos, de forma que permitan el cumplimiento de la finalidad por las que motivaron su gestión.

F. PRINCIPIO DE PROPORCIONALIDAD

Se deberá utilizar los Datos Personales que sean necesarios, adecuados y relevantes, acorde a la finalidad con las que fueron recabados.

G. PRINCIPIO DE INFORMACIÓN

Las áreas que realicen tratamiento de Datos Personales deben informar al Titular, por medio del aviso de privacidad, las características y gestión del tratamiento de sus Datos Personales, de forma que pueda realizar decisiones informadas al respecto.

H. PRINCIPIO DE RESPONSABILIDAD

Los responsables del tratamiento de Datos Personales deberán asegurarse de verificar el cumplimiento de los principios y obligaciones de la LGPDPPSO, adoptando las medidas necesarias para ello, y manifestar ante titulares y autoridades el cumplimiento de la normatividad de Datos Personales.

7. DEBERES

A. DEBER DE SEGURIDAD

Para cumplir con el deber de Seguridad, las Unidades Administrativas del CIAD, se aseguraran de establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de Datos Personales, independientemente del tipo de sistema en el que se encuentren, con el fin de proteger la información contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, buscando garantizar la confidencialidad, integridad y disponibilidad, conforme a los artículos 31, 32, 33, 34, 35, y 36 de la LGPDPPSO, y artículos 55 al 65 de los Lineamientos Generales.

B. DEBER DE CONFIDENCIALIDAD

El personal que integre las Unidades Administrativas del CIAD, deberá establecer controles o mecanismos que tengan por objeto que todos los servidores públicos que intervengan en cualquier fase del tratamiento de los Datos Personales, guarden confidencialidad respecto de éstos, obligación que deberá subsistir aún después de

finalizar sus relaciones con el CIAD, lo anterior deberá ser conforme al artículo 42 de la LGPDPPSO y Artículo 71 de los Lineamientos Generales.

8. VULNERACIONES DE DATOS PERSONALES

En caso de una vulneración a la seguridad, la Unidad Administrativa responsable deberá analizar las causas por las que se presentó, e implementar acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los Datos Personales si fuese el caso a efecto de evitar que la vulneración se repita.

Se considerarán como vulneraciones de seguridad:
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

El CIAD deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa a la misma, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva, en caso de que las vulneraciones afecten de forma significativa los derechos patrimoniales o morales, la Unidad Administrativa responsable deberá informar de forma inmediata al titular de la Unidad de Transparencia.

Entendiéndose como daño a los derechos patrimoniales del titular cuando la vulneración esté relacionada, de forma enunciativa pero no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular. En el caso de la afectación a los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa pero no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.
La Unidad Administrativa responsable deberá notificar al titular de la Unidad de Transparencia las vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular dentro de un plazo máximo de setenta y dos horas, a partir de que confirme la ocurrencia de éstas y responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

9. EVALUACIONES DE IMPACTO DE PROTECCIÓN DE DATOS PERSONALES

El CIAD deberá realizar evaluación en la protección de Datos Personales, en los casos donde se pretenda realizar una operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o

cualquier tecnología que, de conformidad con la LGPDPPSO, pudiera implicar un tratamiento intensivo o relevante de Datos Personales.
Se está en presencia de este tipo de tratamiento cuando:

I. Existan riesgos inherentes a los datos personales a tratar;
II. Se traten datos personales sensibles, y
III. Se efectúen o pretendan efectuar transferencias de datos personales.

Siempre que se pretenda realizar una operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier tecnología que de conformidad con la LGPDPPSO, pudiera implicar un tratamiento intensivo o relevante de Datos Personales, se deberá realizar una evaluación de impacto en la protección de Datos Personales y presentarla ante el INAI treinta días anterior a la fecha en que se pretenda modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier tecnología.
Lo anterior con el fin de que el INAI emita recomendaciones vinculantes sobre la Evaluación de impacto en la protección de Datos Personales

10. DERECHOS DEL TITULAR

A. INFORMACIÓN

El CIAD al momento de recabar la información del titular, deberá hacerlo por medio del aviso de privacidad, haciendo conocedor al titular de la existencia y características principales del tratamiento al que será sometidos sus Datos Personales, para que el aviso de privacidad cumpla de manera eficiente su función de informar, deberá estar redactado y estructurado de forma clara y sencilla.

Lo anterior con el objetivo de hacer saber al titular de lo siguiente:

I. La denominación del responsable;
II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar quienes se transfieren dichos datos y la finalidad de la transferencia;

IV. Los mecanismos y medios disponibles para que el 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;

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

De igual forma, el aviso de privacidad integral, además de lo dispuesto en las anteriores fracciones, debe contener la siguiente información:

I. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;

II. El fundamento legal que faculta para llevar a cabo el tratamiento;

III. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;

IV. El domicilio de la Unidad de Transparencia;

V. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

11. EJERCICIO DE DERECHOS ARCO

Aquellos derechos que posee el o la titular de los Datos Personales, para solicitar el Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de sus datos.

A. ACCESO

Derecho del titular para acceder a sus Datos personales en posesión del CIAD, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

B. RECTIFICACIÓN

Derecho del titular a solicitar al CIAD la rectificación o corrección de sus Datos Personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

C. CANCELACIÓN

Derecho del titular para solicitar la cancelación de sus Datos Personales de los archivos, registros, expedientes y sistemas del CIAD, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

D. OPOSICIÓN

Derecho del titular para oponerse al tratamiento de sus datos personales, o exigir que se cese el mismo, con el propósito de evitar un daño o perjuicio

12. MODALIDADES DE SOLICITUDES

Las solicitudes de ejercicio de derechos ARCO podrá ser realizadas por el titular de los Datos Personales, o por su representante legal, o en el caso de menores de edad o personas en estado de interdicción, por un padre o un tutor legal.

La solicitud para el ejercicio de derechos ARCO requerirá los siguientes requisitos:

I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;

II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;

III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;

IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;

V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y

VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

El CIAD deberá llevar un registro de las solicitudes de ejercicio de derechos ARCO.

13. PLAZOS

La respuesta a las solicitudes del ejercicio de Derechos ARCO no deberá exceder el plazo de veinte días hábiles contados a partir del día siguiente a la recepción de la solicitud, dicho plazo podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en su caso de poder determinar, orientarlo hacia el responsable competente.

En caso de que la solicitud de datos no satisfaga algunos de los requisitos antes mencionados, y el CIAD no cuente con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de los derechos ARCO, por una sola ocasión, para que subsane las omisiones

dentro de un plazo de diez días contados a partir del día siguiente de la notificación, en caso de transcurrir el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de derechos ARCO.

Cuando los lineamientos aplicables al tratamiento de Datos Personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de derechos ARCO, el responsable deberá informar al titular sobre la existencia del mismo en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO.

14. IMPROCEDENCIA DE LAS SOLICITUDES

El ejercicio de los derechos ARCO sólo será improcedente en los siguientes casos:

I. Cuando el titular o su representante no estén debidamente acreditados para ello;

II. Cuando los datos personales no se encuentren en posesión del responsable;

III. Cuando exista un impedimento legal;

IV. Cuando se lesionen los derechos de un tercero;

V. Cuando se obstaculicen actuaciones judiciales o administrativas;

VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;

VII. Cuando la cancelación u oposición haya sido previamente realizada;

VIII. Cuando el responsable no sea competente;

IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;

X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;

XI. Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o

XII. Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

Ante la negativa de dar trámite a toda solicitud para el ejercicio de derechos ARCO, o por falta de respuesta del responsable, procederá la interposición del recurso de revisión, acorde al artículo 94 de la LGPDPPSO.

15. RECURSO DE REVISIÓN

En caso de inconformidad por la respuesta a la solicitud de información por parte del CIAD o por falta de respuesta dentro del plazo establecido, el titular, o por medio de su representante, podrán interponer un recurso de revisión ante el INAI o la Unidad de Transparencia responsable que haya conocido de la solicitud para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del día siguiente a la fecha de notificación de la respuesta.

El recurso de revisión será procedente dentro de los siguientes supuestos:

I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
II. Se declare la inexistencia de los datos personales;
III. Se declare la incompetencia por el responsable;
IV. Se entreguen datos personales incompletos;
V. Se entreguen datos personales que no correspondan con lo solicitado;
VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales;
VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia;
VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;
IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;
X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;
XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y
XII. En los demás casos que dispongan las leyes.

16. PROCESAMIENTO DE DATOS POR PARTE DE LOS ENCARGADOS

El encargado es toda persona física o jurídica, encomendada para el tratamiento de Datos Personales a nombre del CIAD, de modo que, deberá realizar dichas actividades de gestión de Datos Personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable.

RELACIÓN ENTRE EL CIAD Y ENCARGADO

La relación entre responsable y encargado deberá estar formalizada mediante contrato o cualquier instrumento jurídico que decida el responsable, de conformidad con la normativa que resulte aplicable, y que permita acreditar su existencia, alcance y contenido, dicho instrumento deberá prever las siguientes clausulas:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
IV. Informar al responsable 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 responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Los acuerdos entre responsable y encargado relacionados con el tratamiento de Datos Personales no deberá contravenir la presente Ley y demás normatividad aplicable.

SUBCONTRATACIÓN

Siempre y cuando medie la autorización expresa del CIAD, el encargado podrá subcontratar servicios que impliquen el tratamiento de Datos Personales a cuenta del CIAD, el subcontratado asumirá el carácter de encargado en los términos de la presente política y demás normatividad aplicable en la materia.

TERMINACIÓN DE LA RELACIÓN JURÍDICA

Una vez terminada la relación jurídica con el CIAD, el encargado deberá eliminar o entregar los Datos Personales objeto del tratamiento, salvo disposición contraria expresa en la ley.

17. TRANSFERENCIAS DE DATOS PERSONALES

La Transferencia es toda comunicación de Datos Personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al servidor público responsable}, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

A. TRANSFERENCIA NACIONAL

En el caso de una Transferencia Nacional, el receptor de los Datos Personales deberá tratar los Datos Personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos, atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

B. TRANSFERENCIA INTERNACIONAL

En el caso de una Transferencia Internacional, el responsable sólo podrá transferir o hacer remisión de Datos Personales fuera del territorio nacional cuando el tercero receptor o encargado se obligue a proteger los Datos Personales acorde a los principios y deberes establecidos en la LGPDPPSO y toda normatividad que resulte aplicable.

Las transferencias de Datos Personales pueden ser realizadas sin el consentimiento del titular en los siguientes supuestos:

I. Cuando la transferencia esté prevista en esta Ley 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 responsable y el titular;

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

VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente Ley, o

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

Las remisiones nacionales e internacionales de Datos Personales que se realicen entre el responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.

18. MEDIDAS DE APREMIO Y RESPONSABILIDADES

A. MEDIDAS DE APREMIO

El INAI, con el fin de asegurar el cumplimiento de sus determinaciones, podrán imponer las siguientes medidas de apremio:

I. La amonestación pública, o

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

El incumplimiento de los Sujetos Obligados será difundido en los portales de obligaciones de transparencia del INAI y considerados en las evaluaciones que realicen estos.

Si a pesar de la ejecución de las medidas de apremio antes mencionadas, no se cumpliere con la resolución, se requerirá al superior jerárquico el cumplimiento, para que en un plazo no mayor a cinco días, se obligue a cumplir. Transcurrido el plazo, sin que haya cumplimiento, se dará vista a la autoridad competente en materia de responsabilidades.

Las medidas de apremio serán aplicadas por el INAI ya sea por sí mismos o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas. Las multas que fije el INAI se harán efectivas por el Servicio de Administración a través de procedimientos establecidos por la ley.

19. SANCIONES

Conforme a lo estipulado en el artículo 163 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, serán causas de sanción por incumplimiento en las obligaciones 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 presente Ley 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 presente Ley;

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 presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. 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 presente Ley;

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

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 presente Ley;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

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 presente Ley;

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.

Para las conductas anteriormente estipuladas, se dará vista a la autoridad competente para que imponga o ejecute la sanción.

En aquellos casos donde el presunto infractor tenga la calidad de servidor público, el CIAD deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un expediente que contenga todos los elementos que sustenten la presunta responsabilidad administrativa.

La autoridad que conozca del asunto deberá informar de la conclusión del procedimiento y, en su caso, de la ejecución de la sanción.

20. Vigencia

La presente política entrará en vigor a partir de su autorización por parte del Comité de Transparencia.