MOVIMIENTO CIUDADANO

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

(TOMADA DE LA MANO)

ROBERTO MANCILLA

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

(TOMADA DE LA MANO)

INDICE GENERAL

INTRODUCCIÓN

En mi ejercicio profesional como abogado, me ha tocado ver muchas legislaciones con comentarios hechos por otros profesionales y son de gran utilidad (para el especialista), pero lo que aún no he visto es que alguien haga una legislación para explicar las cosas a la población general. Los abogados nos enorgullecemos mucho de lo técnico de nuestra profesión, pero a veces pienso que no somos conscientes sobre la importancia de entender, entre todos, las reglas que rigen el comportamiento colectivo.

Bajo esta premisa, lo que intento llevar a cabo, en esta ocasión, es explicar la Ley General de Datos Personales en Posesión de Sujetos obligados de la misma forma como lo hice con la Ley General de Transparencia y Acceso a la Información Pública: explicaré cada título de la Ley y pondré, en cada artículo y párrafo, un enunciado que resuma su contenido de forma que, al leer cualquier numeral, se tiene un entendimiento casi inmediato.

La idea subyacente en todos los materiales didácticos que hemos producido es que el tema de los datos personales y su protección sea lo más entendible para que ser utilizado por la ciudadanía en la defensa de sus derechos. Los datos personales son un componente esencial de la vida social en la Era digital. Nuestros datos personales son una extensión de nosotros mismos, pero al mismo tiempo pueden estar en manos de otro sin que medie nuestro consentimiento, incluso pueden usarse de formas distintas a las que dimos autorización.

Esta legislación simplificada es meramente un granito de arena en busca de un entendimiento mayor acera de lo que nos rodea; entre más gente sepa usar efectivamente estas herramientas, mejor. Sinceramente espero que sea de utilidad para quien la lea y si alguien la llegara a usar, para explicar todo este fenómeno en una clase del tema (sea al nivel que sea), me sentiré profundamente honrado.

ATENTAMENTE,
ROBERTO MANCILLA
Presidente de la Comisión Nacional de Transparencia de Movimiento Ciudadano, doctor en Derecho por la Universidad de California, Berkeley, y nacido en 1986.

ESTUDIO INTRODUCTORIO A LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

En lo que respecta a los datos personales, su tratamiento y protección, existen dos leyes y éstas tienen distintos ámbitos de aplicación: la Ley Federal de Protección a los Datos Personales en Posesión de Particulares, para particulares como empresas y bancos, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que se aplica al gobierno, entendido éste como las autoridades federales, estatales, municipales (incluidos ayuntamientos, órganos autónomos y los tres poderes), además de partidos políticos, fideicomisos y fondos públicos. Y, por si acaso, se incluye a sindicatos y "cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal."

En México, los datos personales tienen su primer antecedente en la reforma al artículo 6° de la Constitución Política de los Estados Unidos Mexicanos de fecha 6 de diciembre de 1977, cuando se establece el derecho a la información. También resulta importante la publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en junio de 2002, pues es aquí cuando se realiza la primera regulación de datos personales.

En 2007, se profundiza el contenido del artículo 6°, donde se reconoce la protección de la vida privada y los datos personales. En junio de 2009, se reformó el artículo 16 constitucional para reconocer en la Ley Suprema los derechos ARCO. Esto quedó plasmado de la forma siguiente:

> *Artículo 16. (...)]: Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (...)*

El 5 de julio de 2010 se hace una legislación de protección de datos personales aplicable sólo a los particulares: la Ley Federal de Protección a los Datos Personales en Posesión de Particulares. En 2013 y 2016, se reforma nuevamente el artículo 6º constitucional, creando un "apartado A," el cual rige el "ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias."

Ahora bien, existe para los partidos políticos un nuevo régimen de protección de datos personales con la Ley de Datos Personales en Posesión Sujetos Obligados, y empezó a tener revisiones vinculantes por parte del INAI y los garantes locales a partir del verano de 2017. Desde la perspectiva de un partido político se deben implementar tres tipos de medidas de seguridad:

- **Medidas de seguridad administrativas:** políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, todo en materia de protección de datos personales. Un ejemplo de esto lo podemos encontrar en las reglas internas de una organización y la capacitación impartida al personal administrativo que maneja datos personales.
- **Medidas de seguridad físicas:** conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Se deben considerar las siguientes actividades: a) prevenir el acceso no autorizado al perímetro de la organización; b) prevenir daño o interferencia a las instalaciones físicas, recursos e información; c) proteger recursos móviles y portátiles; d) proveer mantenimiento a los equipos que contienen o almacenan datos personales. En este rubro, se tienen, como ejemplo, las inspecciones y evaluaciones de impacto que permiten saber qué sistemas existen en materia de datos y cómo resguardarlos mejor.
- **Medidas de seguridad técnicas:** conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Para ello, se deben considerar los siguientes puntos: a) el acceso a las bases de datos o a la información debe llevarse a cabo por usuarios identificados y autorizados; b) generar un esquema de privilegios para que los usuarios cumplan sus funciones; c) revisar la configuración de seguridad; d) gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos. Esta última medida implica revisar que los datos personales en soporte electrónico estén propiamente resguardados.

Además de las dos leyes que regulan los datos personales en el ámbito nacional, debemos tomar en cuenta que cada entidad federativa tiene una ley de datos personales que aplica (junto con la Ley General) a los sujetos obligados estatales y municipales. Para dar sentido acerca de qué ley aplica en este proceso, el ciudadano puede acudir a una regla sencilla: cuando se quiera ejercer los derechos ARCO sobre un órgano federal, se debe leer la Ley General; cuando se trate del uso de derechos ARCO sobre datos personales en posesión del gobierno estatal o municipal, se debe consultar primero a la Ley General y luego la de la entidad tratada.

Teniendo este marco mínimo, creemos que estamos en condición de estudiar y entender los 168 artículos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los cuales se encuentran repartidos en 11 títulos.

TÍTULO PRIMERO
DISPOSICIONES GENERALES

La Ley General de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO) está compuesta por 11 títulos y 168 artículos; los primeros tratan la división general de esta la Ley y los segundos son la unidad más pequeña que puede tener una Ley. Lo anterior, es una relación similar entre una palabra con un enunciado o un enunciado con un párrafo. Por lo general, las divisiones probables de la legislación son las siguientes: 1. Libros; 2. Títulos, 3 Capítulos y 4. Secciones. La forma en cómo éstas se usen depende del tamaño de la Ley y la cantidad de temas manejados.

Por lo general, toda legislación comienza con un capítulo o título sobre cómo los conceptos básicos aplican en el resto del cuerpo normativo. Esto es muy importante porque en dicha parte se explican cosas como la finalidad de la ley, las personas a quienes se les aplica, los principios que la rigen y los conceptos más relevantes. Es decir, se trata de la brújula que nos ayudará a navegar en la Ley General.

En esta ley, el título de disposiciones generales tiene dos capítulos: el primero, "Objeto de la Ley," establece lo que trata de hacer y el alcance que tiene; en el segundo, "Del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales," nos dice cómo se relaciona el Sistema Nacional de Transparencia creado en la Ley General de Transparencia y Acceso a la Información Pública con los datos personales.

El artículo primero señala la naturaleza de la ley que estamos analizando, "de orden público y de observancia general," es decir, los datos personales y su protección forman parte del funcionamiento normal de la República y debe ser del conocimiento de todos (ciudadanos y autoridades). Es reglamentaria toda ley que amplíe el contenido de la Constitución, en este caso versa del artículo 6º, en específico, la "protección de datos personales en posesión de sujetos obligados."

También se establece en este artículo la aplicabilidad de la Ley, es decir, a quiénes

se les aplica y cómo el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales tiene facultades en materia de datos personales sin importar la que les de la Ley General de Transparencia y Acceso a la Información Pública (en lo sucesivo, LGTAIP).

Se establece también la finalidad ("objeto") de la Ley: "establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados." De la misma forma como sucede con la LGTAIP, se señala quiénes son sujetos obligados: los tres poderes federales y locales, autoridades municipales, partidos políticos, fideicomisos, sindicatos y fondos públicos y se siguen los mismos dos criterios residuales en los que pueden caber otros sujetos no previstos de forma expresa: cualquier persona física o moral que 1) reciba y ejerza recursos públicos o 2) realice actos de autoridad.

Por último, este artículo señala que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares debe aplicar en todos los casos que no haya previsto la LGPDPSO y que, en todo caso, consiste en los sujetos diversos que se señalaron en el artículo 1º.

El artículo 2 establece los objetivos de la LGPDPSO: distribuir las competencias (lo que una autoridad puede o no hacer) en el tema entre los organismos garantes (el órgano que debe cuidar el buen uso de los datos personales) de diversos niveles (local o federal), establecer las bases mínimas que deben operar para todos en la materia, regular el Sistema Nacional de Transparencia en lo relativo a datos personales, obligar que se cumplan los principios básicos, proteger datos personales, garantizar el derecho de protección de datos, promover, fomentar y difundir una cultura de protección de datos personales, así como establecer sanciones que permitan el cumplimiento de la Ley y regular la interposición de acciones de inconstitucionalidad y controversias constitucionales.

El artículo 3º establece las definiciones, una suerte de glosario que permite conocer y reforzar los conceptos primordiales manejados por la Ley. Se trata también la aplicabilidad de la Ley en cuanto a soporte de los datos; es decir, la Ley aplica al tratamiento de datos que estén en medios físicos o digitales (artículo 4º). El artículo 5º señala como fuentes de acceso público (los medios donde se puede encontrar información que es disponible a la población en general) a páginas de Internet, medios de comunicación electrónica, directorios telefónicos, diarios, gacetas o boletines oficiales, medios de comunicación social y registros públicos. Se establecen también criterios para determinar qué se puede considerar como fuente acceso público, para los casos no previstos.

El artículo 6º establece que la privacidad la garantiza el Estado y una serie de limitantes: seguridad nacional, disposiciones de orden público, seguridad y salud

públicas y los derechos de terceros. Complementando lo anterior, el artículo 7º establece una prohibición del tratamiento de datos personales sensibles, siendo la excepción solamente los casos que prevé el artículo 22; asimismo, se establece cómo el tratamiento de datos personales debe privilegiar el interés superior de la niñez y adolescencia: siempre tratar a niños y adolescentes de la forma más favorable posible, cuidando su vulnerabilidad.

El artículo 8º establece el marco normativo aplicable: la Constitución, los tratados internacionales (si son de derechos humanos se les da grado constitucional por el artículo 1º constitucional), así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados. Se repite también el principio pro persona (la interpretación de la ley debe favorecer lo más posible a la persona titular de datos personales y su privacidad) en materia de datos personales. También se establece cómo los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales, son referentes interpretativos (puntos de referencia a la hora de interpretar).

El artículo 9º establece al Código Federal de Procedimientos Civiles y a la Ley Federal de Procedimiento Administrativo como legislaciones supletorias; es decir, son las leyes para suplir las deficiencias presentes en la Ley o para trabajar con los imprevistos que puedan darse. Aunque no lo señala de forma expresa, la LGTAIP también puede ser ley supletoria, toda vez que ésta establece buena parte de la estructura orgánica que se utiliza en materia de datos personales.

En el artículo 10º, se debe considerar un complemento de lo dicho en la Ley General de Transparencia sobre el Sistema Nacional de Transparencia, pues se remite a dicha ley para establecer cuáles son sus facultades en materia de protección de datos personales, además de señalar de nueva cuenta a dicha legislación como aplicable. El artículo 11º sigue esta lógica al señalar los objetivos del sistema y los mecanismos a su alcance para cumplir sus objetivos.

Se establece que debe existir un Programa Nacional para la Protección de Datos Personales, diseñado por el Sistema Nacional de Transparencia y se plantean sus funciones y objetivos: fomento cultural y del ejercicio de derechos, capacitación de sujetos obligados, creación y mantenimiento de un sistema de gestión de seguridad, además de medir y verificar las metas establecidas, determinar y jerarquizar los objetivos y metas a cumplir y definir las líneas de acción generales que resulten necesarias, entre otras (Artículo 12).

Se establece cómo el Sistema Nacional deberá contar con un Consejo y, de forma más clara, las funciones que debe tener el Sistema Nacional en materia de datos personales, aun y cuando habían sido mayormente señaladas en el artículo 12. Éstas son: promover el ejercicio del derecho a la protección de datos personales, fomento

cultural, proponer cambios a las leyes, establecer mecanismos de coordinación, emitir acuerdos y resoluciones generales; crear y ejecutar políticas generales de datos personales, coordinar las instancias que integran el Sistema, homologar y desarrollar los procedimientos previstos en la ley, diseñar políticas específicas de datos personales; establecer mecanismos de participación ciudadana, desarrollar proyectos para medir el alcance de los responsables, suscribir convenios de colaboración, crear e implementar acciones para garantizar la accesibilidad de grupos vulnerables, proponer códigos de buenas prácticas, reglas o modelos; comunicarse con otros niveles de gobierno y organismos internacionales, vincular el Sistema Nacional con otros sistemas, implementar y operar la Plataforma Nacional, aprobar el Programa Nacional de Protección de Datos Personales, expedir criterios, expedir disposiciones administrativas, y otras cosas que se establezcan en leyes diversas a esta (a esto se le conoce como cláusula residual) (Artículo 14).

Por último, el artículo 15 señala la legislación que resulta aplicable al Consejo del Sistema Nacional de Transparencia, en este caso, la Ley General de Transparencia y Acceso a la Información Pública, cosa que ya se infirió de artículos pasados.

CAPÍTULO I
DEL OBJETO DE LA LEY

NATURALEZA

Artículo 1. La presente Ley es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

APLICABILIDAD DE LA LEY EN CUANTO AL ORDEN DE GOBIERNO

Todas las disposiciones de esta Ley General, según corresponda, y en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

ATRIBUCIONES DEL INSTITUTO EN MATERIA DE DATOS PERSONALES

El Instituto ejercerá las atribuciones y facultades que le otorga esta Ley, independientemente de las otorgadas en las demás disposiciones aplicables.

OBJETO DE LA LEY

Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

SUJETOS OBLIGADOS

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

SUJETOS OBLIGADOS (CONT.)

Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

LEGISLACIÓN COMPLEMENTARIA

En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

OBJETIVOS DE LA LEY. ENUMERACIÓN

Artículo 2. Son objetivos de esta Ley:

I. Distribución Competencial: Distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados;

II. Bases Mínimas y Homologación: Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;

III. Regular el Sistema Nacional de Transparencia en lo relativo a datos personales: Regular la organización y operación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refieren esta Ley y la Ley General de Transparencia y Acceso a la Información Pública, en lo relativo a sus funciones para la protección de datos personales en posesión de sujetos obligados;

IV. Garantizar la observancia de principios básicos: Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;

V. Proteger datos personales: Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento;

VI. Garantizar el derecho de protección de datos: Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;

VII. Promover, fomentar y difundir una cultura de protección de datos personales: Promover, fomentar y difundir una cultura de protección de datos personales;

VIII. Establecer un régimen sancionador: Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley, y

IX. Establecer medios de impugnación: Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes locales y de la Federación; de conformidad con sus facultades respectivas.

DEFINICIONES

Artículo 3. Para los efectos de la presente Ley se entenderá por:

I. Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

II. 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 los mismos;

III. Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

IV. Bloqueo: La identificación y conservación de datos personales una vez cumplida 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 en la base de datos que corresponda;

V. Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;

VI. Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en

recursos compartidos dinámicamente;

VII. Consejo Nacional: Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refiere el artículo 32 de la Ley General de Transparencia y Acceso a la Información Pública;

VIII. Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

IX. 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;

X. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual **(tipos de datos sensibles)**;

XI. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

XII. Días: Días hábiles;

XIII. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

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

XV. Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

XVI. Evaluación de impacto en la protección de datos personales: Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;

XVII. Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;

XVIII. Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;

XIX. Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

XX. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XXI. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

XXII. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades **(tipos de medidas):**

a) Prevenir el acceso no autorizado al perímetro de la organización: Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir daño o interferencia a las instalaciones físicas, recursos e información: Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger recursos móviles y portátiles: Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer mantenimiento a los equipos que contienen o almacenan datos personales: Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

XXIII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades **(tipos de medidas técnicas):**

a) Que el acceso a las bases de datos o a la información sea por usuarios identificados y autorizados: Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que los usuarios cumplan sus funciones: Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad: Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos: Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

XXIV. Organismos garantes: Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales, en términos de los artículos 6o. y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos;

XXV. Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;

XXVI. Programa Nacional de Protección de Datos Personales: Programa Nacional de Protección de Datos Personales;

XXVII. Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

XXVIII. Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;

XXIX. Sistema Nacional: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XXX. Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

XXXI. Titular: La persona física a quien corresponden los datos personales;

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

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

XXXIV. Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

APLICABILIDAD DE LA LEY EN CUANTO A SOPORTE DE LOS DATOS

Artículo 4. La presente Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

FUENTES DE ACCESO PÚBLICO

Artículo 5. Para los efectos de la presente Ley, se considerarán como fuentes de acceso público:

I. Páginas de Internet y medios de comunicación electrónica: Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;

II. Directorios telefónicos: Los directorios telefónicos en términos de la normativa específica;

III. Diarios, gacetas o boletines oficiales: Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;

IV. Medios de comunicación social: Los medios de comunicación social, y

V. Registros públicos: Los registros públicos conforme a las disposiciones que les resulten aplicables.

CRITERIO PARA DETERMINAR EL ACCESO PÚBLICO

Para que los supuestos enumerados en el presente artículo sean considerados fuentes

de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contra prestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita **(límite).**

GARANTÍA A LA PRIVACIDAD POR PARTE DEL ESTADO

Artículo 6. El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

LÍMITES A LA PRIVACIDAD

El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

PROHIBICIÓN DE LA TRATA DE DATOS PERSONALES SENSIBLES

Artículo 7. Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley **(excepción)**.

INTERÉS SUPERIOR DE LA NIÑEZ Y ADOLESCENCIA

En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables.

MARCO NORMATIVO APLICABLE

Artículo 8. La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia **(principios interpretativos)**.

REFERENTES INTERPRETATIVOS

Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

LEGISLACIÓN SUPLETORIA

Artículo 9. A falta de disposición expresa en la presente Ley, se aplicarán de manera supletoria las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo.

LEGISLACIÓN SUPLETORIA EN LAS ENTIDADES FEDERATIVAS

Las leyes de las Entidades Federativas, en el ámbito de sus respectivas competencias, deberán determinar las disposiciones que les resulten aplicables en materia supletoria a los Organismos garantes en la aplicación e interpretación de esta Ley.

CAPÍTULO II

DEL SISTEMA NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

SISTEMA NACIONAL

Artículo 10. El Sistema Nacional se conformará de acuerdo con lo establecido en la Ley General de Transparencia y Acceso a la Información Pública **(conformación)**. En materia de protección de datos personales, dicho Sistema tiene como función coordinar y evaluar las acciones relativas a la política pública transversal de protección de datos personales, así como establecer e implementar criterios y lineamientos en la materia **(Función del Sistema en materia de datos personales),** de conformidad con lo señalado en la presente Ley, la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable **(Legislación aplicable).**

OBJETIVOS

Artículo 11. El Sistema Nacional contribuirá a mantener la plena vigencia del derecho a la protección de datos personales a nivel nacional, en los tres órdenes de gobierno.

MECANISMOS PARA CUMPLIR SUS OBJETIVOS

Este esfuerzo conjunto e integral, aportará a la implementación de políticas públicas con estricto apego a la normatividad aplicable en la materia; el ejercicio pleno y respeto del derecho a la protección de datos personales y la difusión de una cultura de este derecho y su accesibilidad.

PROGRAMA NACIONAL PARA LA PROTECCIÓN DE DATOS PERSONALES

Artículo 12. Además de los objetivos previstos en la Ley General de Transparencia y Acceso a la Información Pública, el Sistema Nacional tendrá como objetivo diseñar, ejecutar y evaluar un Programa Nacional de Protección de Datos Personales que defina

la política pública y establezca, como mínimo, objetivos, estrategias, acciones y metas para **(objetivos del Programa):**

I. Fomento cultural: Promover la educación y una cultura de protección de datos personales entre la sociedad mexicana;

II. Fomento del ejercicio de derechos: Fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición;

III. Capacitación: Capacitar a los sujetos obligados en materia de protección de datos personales;

IV. Sistema de gestión de seguridad: Impulsar la implementación y mantenimiento de un sistema de gestión de seguridad a que se refiere el artículo 34 de la presente Ley, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia, y

V. Medición y verificación de las metas: Prever los mecanismos que permitan medir, reportar y verificar las metas establecidas.

FUNCIÓN DEL PROGRAMA

El Programa Nacional de Protección de Datos Personales, se constituirá como un instrumento rector para la integración y coordinación del Sistema Nacional, y deberá determinar y jerarquizar los objetivos y metas que éste debe cumplir, así como definir las líneas de acción generales que resulten necesarias.

EVALUACIÓN Y ACTUALIZACIÓN DEL PROGRAMA

El Programa Nacional de Protección de Datos Personales deberá evaluarse y actualizarse al final de cada ejercicio anual y definirá el conjunto de actividades y proyectos que deberán ser ejecutados durante el siguiente ejercicio.

CONSEJO DEL SISTEMA NACIONAL

Artículo 13. El Sistema Nacional contará con un Consejo Nacional. En la integración, organización, funcionamiento y atribuciones del Consejo Nacional se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables.

FUNCIONES DEL SISTEMA NACIONAL EN MATERIA DE DATOS PERSONALES

Artículo 14. El Sistema Nacional, además de lo previsto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable, tendrá las

siguientes funciones en materia de protección de datos personales:

I. Promover el ejercicio del derecho a la protección de datos personales: Promover el ejercicio del derecho a la protección de datos personales en toda la República Mexicana;

II. Fomento cultural: Fomentar entre la sociedad una cultura de protección de los datos personales;

III. Proponer cambios a las leyes: Analizar, opinar y proponer a las instancias facultadas para ello proyectos de reforma o modificación de la normativa en la materia;

IV. Establecer mecanismos de coordinación: Acordar y establecer los mecanismos de coordinación que permitan la formulación y ejecución de instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendentes a cumplir con los objetivos y fines del Sistema Nacional, de la presente Ley y demás disposiciones que resulten aplicables en la materia;

V. Emitir acuerdos y resoluciones generales: Emitir acuerdos y resoluciones generales para el funcionamiento del Sistema Nacional;

VI. Crear y ejecutar políticas generales de datos personales: Formular, establecer y ejecutar políticas generales en materia de protección de datos personales;

VII. Coordinar las instancias que integran el Sistema: Promover la coordinación efectiva de las instancias que integran el Sistema Nacional y dar seguimiento a las acciones que para tal efecto se establezcan;

VIII. Homologar y desarrollar: Promover la homologación y desarrollo de los procedimientos previstos en la presente Ley y evaluar sus avances;

IX. Diseñar políticas específicas de datos personales: Diseñar e implementar políticas en materia de protección de datos personales;

X. Establecer mecanismos de participación ciudadana: Establecer mecanismos eficaces para que la sociedad participe en los procesos de evaluación de las políticas y las instituciones integrantes del Sistema Nacional;

XI. Desarrollar proyectos para medir el alcance de los responsables: Desarrollar proyectos comunes de alcance nacional para medir el cumplimiento y los avances de los responsables;

XII. Suscribir convenios de colaboración: Suscribir convenios de colaboración que tengan por objeto coadyuvar al cumplimiento de los objetivos del Sistema Nacional y aquellos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;

XIII. Crear e implementar acciones para garantizar la accesibilidad de grupos vulnerables: Promover e implementar acciones para garantizar condiciones de

accesibilidad para que los grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales;

XIV. Proponer códigos de buenas prácticas, reglas o modelos: Proponer códigos de buenas prácticas o modelos en materia de protección de datos personales;

XV. Comunicarse con otros niveles de gobierno y organismos internacionales: Promover la comunicación y coordinación con autoridades nacionales, federales, de los Estados, municipales, autoridades y organismos internacionales, con la finalidad de impulsar y fomentar los objetivos de la presente Ley;

XVI. Vincular el Sistema Nacional con otros sistemas: Proponer acciones para vincular el Sistema Nacional con otros sistemas y programas nacionales, regionales o locales;

XVII. Implementar y operar la Plataforma Nacional: Promover e impulsar el ejercicio y tutela del derecho a la protección de datos personales, a través de la implementación, organización y operación de la Plataforma Nacional, a que se refiere la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable;

XVIII. Aprobar el Programa Nacional de Protección de Datos Personales: Aprobar el Programa Nacional de Protección de Datos Personales al que se refiere el artículo 12 de esta Ley;

XIX. Expedir criterios: Expedir criterios adicionales para determinar los supuestos en los que se está ante un tratamiento intensivo o relevante de datos personales, de conformidad con lo dispuesto por los artículos 70 y 71 de esta Ley;

XX. Expedir disposiciones administrativas: Expedir las disposiciones administrativas necesarias para la valoración del contenido presentado por los sujetos obligados en la Evaluación de impacto en la protección de datos personales, a efecto de emitir las recomendaciones no vinculantes que correspondan, y

XXI. Cláusula residual: Las demás que se establezcan en otras disposiciones en la materia para el funcionamiento del Sistema Nacional.

LEGISLACIÓN APLICABLE AL CONSEJO NACIONAL

Artículo 15. El Consejo Nacional funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás ordenamientos aplicables.

TÍTULO SEGUNDO
PRINCIPIOS Y DEBERES

En el título segundo de esta ley, se habla de los principios que rigen la protección de datos personales y los deberes que constituyen dicho acto. El artículo 17 señala los principios de "licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales," pero no los define. Invariablemente de la interpretación que al efecto haga el INAI o el garante local cuando corresponda, estos principios no son difíciles de entender: la licitud habla de obtener los datos de formas señaladas por la Ley, sin mediar engaño (ver también el artículo 19), y atendiendo al consentimiento de quien es titular del dato personal; la finalidad habla sobre el dato obtenido y cómo éste debe servir para un propósito específico, atendiendo a que lo adquirido sea adecuado a dicho propósito (proporcionalidad). El resguardo en curso de los datos personales debe hacerse en la forma que la Ley determine como correcta, y se debe informar al titular acerca de algún cambio en el estado de la misma.

En los artículos 17 y 18 se establece el principio de legalidad, que nos dice que se debe de actuar dentro las competencias que confiere la Ley y que el tratamiento de datos personales debe de estar debidamente justificado. Lo primero se conoce, dentro de la terminología jurídica como fundamentación y lo segundo como motivación. La justificación debida se debe hacer por medio del aviso de privacidad, que es una comunicación hecha al titular del dato personal donde se le comunica que se pide su dato personal para un propósito determinado y que se requiere de su permiso para obtenerlo y tratarlo.

En el artículo 20, se establecen las reglas necesarias para obtener el consentimiento del titular de los datos, el dual debe ser libre (sin que haya dolo o engaño), específico (con una finalidad determinada y licita) e informado (el titular de los datos personales debe saber la finalidad del uso de sus datos antes de otorgar permiso). Además, se establecen las reglas para la obtención del consentimiento de menores de edad o personas en estado de interdicción.

El permiso que dé el titular de los datos personales para el tratamiento de los mismos por un sujeto obligado de la Ley puede manifestarse de forma expresa (abierta e inequívoca, sea verbal, escrita u otra) o tácita (cuando no existe negativa a que se obtengan y traten los datos, es decir, de forma implícita); esta última forma se presume como buena ("válida", dice la Ley), a menos que exista prueba de lo contrario. Cuando se trata de datos personales sensibles, el consentimiento debe obtenerse de forma expresa y por escrito.

El artículo 22 establece una serie de casos de excepción al consentimiento; es decir, cuando no se necesita permiso para obtener un dato personal: cuando lo establezca la Ley, cuando una autoridad lo transfiera al otro dentro de la capacidad que la Ley les otorga para ello, cuando exista mandato judicial o de autoridad competente, para defender al titular de los derechos, para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable, en situaciones de emergencia, para prestar asistencia sanitaria, cuando los datos personales figuren en fuentes de acceso público, cuando los datos personales se sometan a un procedimiento previo de disociación y en el caso de que se trate de datos de personas reportadas como desaparecidas.

En el artículo 23, se establece la responsabilidad de quien obtiene los datos personales, es decir, la de mantener la veracidad de los datos personales ("exactos, completos, correctos y actualizados"); además se presume que los datos personales obtenidos de forma directa por el titular poseen calidad. También se establece que cuando los datos ya no sean necesarios para la finalidad para la cual se obtuvieron, deben suprimirse, además de un plazo específico (llamado plazo de conservación) para guardar dicha información y ésta debe obedecer a la finalidad para la que se obtuvo.

En el artículo 24, se establecen los procedimientos para la conservación, bloqueo y supresión de datos personales; por otro lado, en el 26 se establece el contenido del aviso de privacidad, los medios para su envío, los requerimientos para su redacción y las medidas compensatorias de comunicación masiva del aviso de privacidad.

En el artículo 27, se establecen las modalidades del aviso de privacidad, es decir, las formas que puede tomar. Se habla de un aviso simplificado cuando se tiene la información mínima para cumplir con el propósito que establece la Ley. Dicha información requerida es la denominación del responsable, las finalidades del tratamiento, la autoridad receptora, la finalidad de la transferencia, los mecanismos y medios para manifestar la negativa al tratamiento y el sitio para consultar el aviso de privacidad. El aviso integral tiene la mayor cantidad de información posible y comprende el domicilio del responsable, los datos personales que serán sometidos a tratamiento, la fundamentación, las finalidades del tratamiento, los mecanismos para ejercer derechos ARCO, el domicilio de la Unidad de Transparencia y los medios para comunicar los cambios al aviso de privacidad.

En el artículo 29, se establece la implementación de mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de Ley y los criterios para el uso de mejores prácticas. Mientras que en el 30 se establecen mecanismos para el cumplimiento de la responsabilidad de resguardo de datos personales y entre los que figuran destinar recursos a programas y políticas de protección de datos, elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización; implementar programas de actualización y capacitación, revisar periódicamente las políticas y programas, establecer un sistema de supervisión y vigilancia, establecer procedimientos para recibir y responder dudas y quejas y en general, el diseño, desarrollo e implementación de "políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales."

El Capítulo II de este título trata de los deberes en el resguardo de los datos personales; es decir, aquí se listan tanto las responsabilidades entendidas como una serie de actividades y medidas concretas que tienen como propósito prevenir la difusión de los datos personales recabados y su caída en malas manos. Esto comienza en el artículo 31 al establecer la obligación de implementar medidas de seguridad para la protección de datos personales. En el artículo 32, se establecen los criterios a considerar por las medidas de seguridad, entre los que encontramos: el riesgo inherente a los datos tratados, la sensibilidad de los datos personales, el desarrollo tecnológico, las posibles consecuencias de una vulneración, la transferencia de los datos que se realicen, el número de titulares, vulneraciones previas y el riesgo por el valor potencial que pudieran tener para una tercera persona no autorizada.

En el artículo 33, se enlistan las actividades para establecer y mantener las medidas de seguridad: crear políticas internas para la gestión y tratamiento de los datos personales, definir las funciones y obligaciones del personal involucrado, elaborar un inventario de datos personales; realizar un análisis de riesgo de los datos personales y uno de brecha, elaborar un plan de trabajo, monitorear y revisar periódicamente las medidas de seguridad implementadas, diseñar y aplicar diferentes niveles de capacitación del personal. Es decir, estas actividades son las medidas necesarias para establecer las medidas de seguridad.

En el artículo 34, se define lo que es el sistema de gestión de medidas de seguridad ("conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales…") y se establecen con claridad sus parámetros ("Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales…"). Asimismo, se instaura uno de los pilares más importantes de las medidas de seguridad de datos personales: el documento de seguridad.

A grandes rasgos, este documento contiene los elementos mínimos que permiten tener una idea clara de cómo se guarda la información, dónde se ha fallado y qué diferencias hay entre las medidas de seguridad existentes y las que pide la Ley. Su contenido es el siguiente (artículo 35): inventario de datos personales y de los sistemas de tratamiento, funciones y obligaciones de las personas que traten datos personales, análisis de riesgos, análisis de brecha, plan de trabajo, mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación.

Debido a que el resguardo de datos es una actividad continua, como lo es también la obtención de los mismos, este documento está sujeto a cambios y a actualizaciones y la ley prevé en el artículo 36 una serie de casos de actualización: Modificaciones por cambios en nivel de riesgo, revisión por mejora continua, mitigación del impacto de una vulneración a la seguridad ocurrida, acciones correctivas y preventivas.

En el artículo 37, se establece un procedimiento estándar para el caso de una vulneración a la seguridad y en el 38, se definen las vulneraciones a la seguridad: la pérdida o destrucción no autorizada del dato personal, el robo, extravío o copia no autorizada, el uso, acceso o tratamiento no autorizado y el daño, la alteración o modificación no autorizada. Si se llega a dar alguno de los supuestos anteriores, se debe registrar debidamente en la bitácora de vulneraciones (artículo 39) a la seguridad y debe realizarse una serie de notificaciones al titular de derechos y a la autoridad correspondiente (artículo 40). El informe que se dé al titular de los datos personales vulnerados (artículo 41) debe contener la naturaleza del incidente, los datos personales comprometidos, recomendaciones al titular sobre medidas que puede tomar para proteger sus intereses, acciones correctivas y medios donde se pueda obtener mayor información.

Por último, el artículo 42 establece el control de confidencialidad: toda medida que tenga por objeto hacer que los actores en la obtención y tratamiento de datos personales no divulguen información respecto a sus actividades, incluso tiempo después de realizada esta actividad. Por lo general, esta medida se implementa por medio de un contrato.

CAPÍTULO I
DE LOS PRINCIPIOS

PRINCIPIOS BÁSICOS

Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

PRINCIPIO DE LEGALIDAD (POR ACTUAR DENTRO DE UNA COMPETENCIA DEFINIDA)

Artículo 17. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

PRINCIPIO DE LEGALIDAD (MOTIVACIÓN)

Artículo 18. Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

REQUISITOS PARA TRATAR DATOS PERSONALES FUERA DEL AVISO DE PRIVACIDAD

El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

DEBER DE ACTUAR DE FORMA LÍCITA

Artículo 19. El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

CONSENTIMIENTO DEL TITULAR DE LOS DATOS

Artículo 20. Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma **(forma en que se otorga):**

I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;

II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e

III. Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

OBTENCIÓN DEL CONSENTIMIENTO DE MENORES DE EDAD O PERSONAS EN ESTADO DE INTERDICCIÓN

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

MANIFESTACIÓN DEL CONSENTIMIENTO

Artículo 21. El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología (definición de consentimiento expreso).

DEFINICIÓN DE CONSENTIMIENTO TÁCITO

El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

PRESUNCIÓN DE VALIDEZ DEL CONSENTIMIENTO TÁCITO (JURIS TANTUM)

Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

CONSENTIMIENTO EN DATOS PERSONALES SENSIBLES

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta Ley.

EXCEPCIONES AL CONSENTIMIENTO

Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

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

II. Transferencias entre autoridades para el uso de sus atribuciones: 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. Mandato judicial o de autoridad competente: Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

IV. Para defender al titular de los derechos: Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

V. Para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable: 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. Situaciones de emergencia: Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VII. Prestación de asistencia sanitaria: 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: Cuando los datos personales figuren en fuentes de acceso público;

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

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

PRESERVACIÓN DE LA VERACIDAD DE LOS DATOS PERSONALES

Artículo 23. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

PRESUNCIÓN DE CALIDAD EN DATOS PERSONALES

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

SUPRESIÓN DE DATOS

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

PLAZOS DE CONSERVACIÓN DE LOS DATOS PERSONALES

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

PROCEDIMIENTOS PARA LA CONSERVACIÓN, BLOQUEO Y SUPRESIÓN DE DATOS PERSONALES

Artículo 24. El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley.

REQUERIMIENTOS MÍNIMOS

En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.

Artículo 25. El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

AVISO DE PRIVACIDAD

Artículo 26. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

MEDIOS PARA SU ENVÍO

Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable.

REQUERIMIENTOS

Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla.

MEDIDAS COMPENSATORIAS DE COMUNICACIÓN MASIVA DEL AVISO DE PRIVACIDAD

Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

MODALIDADES DEL AVISO DE PRIVACIDAD

Artículo 27. El aviso de privacidad a que se refiere el artículo 3, fracción II, se pondrá a disposición del titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información **(contenido del aviso simplificado)**:

I. Denominación del responsable: La denominación del responsable;

II. Finalidades del tratamiento: Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;

III. En caso de transferencia de datos: Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:

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

b) Finalidad de la transferencia: Las finalidades de estas transferencias;

IV. Mecanismos y medios para manifestar la negativa al tratamiento: 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, y

V. Sitio para consultar el aviso de privacidad: El sitio donde se podrá consultar el aviso de privacidad integral.

LA NOTIFICACIÓN DEL AVISO SIMPLIFICADO NO EXIME DE LA PUESTA A DISPOSICIÓN DEL INTEGRAL

La puesta a disposición del aviso de privacidad al que refiere este artículo no exime al responsable de su obligación de proveer los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad al que se refiere el artículo siguiente.

DISPONIBILIDAD DE LOS MECANISMOS PARA LA NEGATIVA

Los mecanismos y medios a los que se refiere la fracción IV de este artículo, deberán estar disponibles para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a que ocurra dicho tratamiento.

CONTENIDO DEL AVISO INTEGRAL

Artículo 28. El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo anterior, al que refiere la fracción V del artículo anterior deberá contener, al menos, la siguiente información:

I. Domicilio del responsable: El domicilio del responsable;

II. Datos personales que serán sometidos a tratamiento: Los datos personales

que serán sometidos a tratamiento, identificando aquéllos que son sensibles;

III. Fundamentación: El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;

IV. Finalidades del tratamiento: Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;

V. Mecanismos para ejercer derechos ARCO: Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;

VI. Domicilio de la Unidad de Transparencia: El domicilio de la Unidad de Transparencia, y

VII. Medios para comunicar los cambios al aviso de privacidad: Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

IMPLEMENTACIÓN DE MECANISMOS PARA ACREDITAR EL CUMPLIMIENTO DE PRINCIPIOS, DEBERES Y OBLIGACIONES DE LEY

Artículo 29. El responsable deberá implementar los mecanismos previstos en el artículo 30 de la presente Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto o a los Organismos garantes, según corresponda, caso en el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines **(criterios para el uso de mejores prácticas)**.

MECANISMOS PARA EL CUMPLIMIENTO

Artículo 30. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

I. Destinar recursos a programas y políticas de protección de datos: Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;

II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización: Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;

III. Implementar programas de actualización y capacitación: Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;

IV. Revisar periódicamente las políticas y programas: Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;

V. Establecer un sistema de supervisión y vigilancia: Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;

VI. Establecer procedimientos para recibir y responder dudas y quejas: Establecer procedimientos para recibir y responder dudas y quejas de los titulares;

VII. Cláusula residual: Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y

VIII. Cláusula residual (cont.): Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

CAPÍTULO II
DE LOS DEBERES

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

Artículo 31. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

CRITERIOS A CONSIDERAR POR LAS MEDIDAS DE SEGURIDAD

Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:

I. Riesgo inherente a los datos tratados: El riesgo inherente a los datos personales tratados;

II. Sensibilidad de los datos personales: La sensibilidad de los datos personales tratados;

III. Desarrollo tecnológico: El desarrollo tecnológico;

IV. Posibles consecuencias de una vulneración: Las posibles consecuencias de una vulneración para los titulares;

V. Transferencia de datos que se realicen: Las transferencias de datos personales que se realicen;

VI. Número de titulares: El número de titulares;

VII. Vulneraciones previas: Las vulneraciones previas ocurridas en los sistemas de tratamiento, y

VIII. Riesgo por el valor potencial que pudieran tener para una tercera persona

no autorizada: El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

ACTIVIDADES PARA ESTABLECER Y MANTENER LAS MEDIDAS DE SEGURIDAD

Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los datos personales: Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado: Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales: Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los datos personales: Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Realizar un análisis de brecha: Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo: Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. Monitorear y revisar periódicamente las medidas de seguridad implementadas: Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal: Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

SISTEMA DE GESTIÓN DE MEDIDAS DE SEGURIDAD

Artículo 34. Las acciones relacionadas con las medidas de seguridad para el tratamiento

de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

DEFINICIÓN DE SISTEMAS DE GESTIÓN

Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

DOCUMENTO DE SEGURIDAD. CONTENIDO

Artículo 35. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

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

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

III. Análisis de riesgos: El análisis de riesgos;

IV. Análisis de brecha: El análisis de brecha;

V. Plan de trabajo: El plan de trabajo;

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

VII. Programa general de capacitación: El programa general de capacitación.

CASOS DE ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

Artículo 36. El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

I. Modificaciones por cambios en nivel de riesgo: Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

II. Revisión por mejora continua: Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Mitigación del impacto de una vulneración a la seguridad ocurrida: Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la

seguridad ocurrida, y

IV. Acciones correctivas y preventivas: Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

MEDIDAS EN CASO DE UNA VULNERACIÓN A LA SEGURIDAD

Artículo 37. En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las 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.

VULNERACIONES A LA SEGURIDAD

Artículo 38. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

I. Pérdida o destrucción no autorizada: La pérdida o destrucción no autorizada;

II. Robo, extravío o copia no autorizada: El robo, extravío o copia no autorizada;

III. Uso, acceso o tratamiento no autorizado: El uso, acceso o tratamiento no autorizado, o

IV. Daño, la alteración o modificación no autorizada: El daño, la alteración o modificación no autorizada.

BITÁCORA DE VULNERACIONES A LA SEGURIDAD

Artículo 39. El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

PROCEDIMIENTO EN CASO DE VULNERACIÓN

Artículo 40. El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

CONTENIDO DEL INFORME AL TITULAR DE LOS DATOS VULNERADOS

Artículo 41. El responsable deberá informar al titular al menos lo siguiente:

I. Naturaleza del incidente: La naturaleza del incidente;

II. Datos personales comprometidos: Los datos personales comprometidos;

III. Recomendaciones al titular: Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;

IV. Acciones correctivas: Las acciones correctivas realizadas de forma inmediata, y

V. Medios donde se pueda obtener mayor información: Los medios donde puede obtener más información al respecto.

CONTROL DE CONFIDENCIALIDAD

Artículo 42. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

TÍTULO TERCERO
DERECHOS DE LOS TITULARES Y SU EJERCICIO

En este título, se analizan los llamados derechos ARCO, consagrados en el artículo 16 constitucional, estos implican el acceso del individuo a obtener información sobre sí mismo en las bases de datos públicas o privadas y a saber cómo es tratada, cuáles son los fines que se persiguen y las fuentes de donde dicha información ha sido tomada; la rectificación que permite a la persona corregir los datos inexactos o incompletos, la cancelación de información considerada como inadecuada o excesiva y la oposición, es decir, permitir a la persona negarse a que se lleve a cabo el tratamiento de sus datos personales o se cese el mismo, en los supuestos y con las excepciones previstas en la Ley.

El artículo 43 establece la posibilidad de ejercer los derechos ARCO, aclarando que el ejercicio de cualquiera de este grupo de derechos no es requisito para ejercer otro ni obstáculo para ello. En el artículo 44, se establece el derecho de acceso a datos personales; en el 45, la rectificación o corrección de datos; en el 46, la cancelación y en el 47, la oposición. Este último derecho puede ejercerse bajo dos supuestos: cuando cause daño o perjuicio (aun siendo licito el tratamiento) y cuando existe un tratamiento automatizado que le produce efectos jurídicos no deseados.

En el capítulo II de este título, se plantea a grandes rasgos el procedimiento para ejercer los derechos ARCO. El ejercicio de estos derechos es gratuito, aunque se pueden cobrar costos de reproducción, certificación y envío cuando lo permita la Ley (artículo 50); se requiere acreditar que es el titular de los datos personales o el representante del mismo (artículo 49). Los procedimientos establecidos deben ser sencillos y no deben exceder en su respuesta los veinte días, aunque se puede ampliar dicho plazo por diez, cuando así lo justifiquen las circunstancias (artículo 51).

Toda solicitud para el ejercicio de los derechos ARCO debe cumplir con los siguientes requisitos: nombre del titular y su domicilio, documentos que acrediten la identidad del titular, el área responsable que trata los datos personales, una descripción clara y precisa de los datos personales, una descripción del derecho ARCO

y cualesquiera otros elementos que faciliten la localización de los datos personales (Artículo 52).

En el caso de una solicitud de acceso, debe señalarse también la modalidad en que se quiere reproducir los datos; para las cancelaciones, se debe señalar las razones de por qué se solicita la supresión del dato y, en el caso de la oposición, se debe de justificar el cese en el tratamiento y el daño o perjuicio que el mismo le causa (Artículo 52).

Si alguno de los requisitos generales o específicos de la solicitud no se cumple o existen defectos en la misma, el INAI o el garante local deberá avisarle al solicitante (en terminología de la Ley, se habla de "prevenir") dentro de cinco días después de hecha la petición, para que corrija la misma dentro de diez. Si no se hace, se tiene por no presentada (Artículo 52).

El procedimiento para tramitar la solicitud de ejercicio de derechos ARCO es el siguiente: se presenta la solicitud ante la Unidad de Transparencia del quien el titular de datos personales considere, la petición puede hacerse por escrito, formatos, vía electrónica u otro medio, pero, al recibir la petición, debe acusarse de recibo. El INAI y los garantes locales pueden hacer formularios o sistemas de métodos simplificados para el ejercicio de derechos ARCO, pero lo que importa es que el procedimiento, cualquiera en cada caso, sea de fácil acceso y de la más amplia cobertura (artículo 52).

Habrá veces que a un responsable de datos personales le llegue una solicitud que no sea de su incumbencia o no tenga capacidad para contestarlo, a esto se le llama incompetencia; en este caso, se debe responder al solicitante en tres días explicando por qué y dirigiéndolo a quien pueda ser competente. Puede pasar también que no exista el dato personal sobre el que se hace la solicitud de derecho ARCO, en ese caso, se debe declarar la existencia o no del mismo por el Comité de Transparencia (artículo 53).

No proceden los derechos ARCO por falta de acreditación, datos que no estén en posesión del responsable, impedimento legal, porque se lesionen derechos de terceros, porque ello implique un obstáculo a la justicia o a la administración; porque lo impida la resolución de autoridad competente, porque haya una cancelación u oposición ya ejercida, porque el responsable es incompetente, porque los datos son necesarios para proteger intereses jurídicamente tutelados del titular; para dar cumplimiento a obligaciones legalmente adquiridas por el titular, para mantener la integridad, estabilidad y permanencia del Estado mexicano, para dar cumplimiento a regulación y supervisión financiera. En cualquier caso, se debe fundamentar y motivar la improcedencia (artículo 55). El titular puede impugnar la negativa a dar trámite a su solicitud o la falta de respuesta a la misma por medio del recurso de revisión previsto por el artículo 94 de la Ley (artículo 56).

Por último, el artículo 57 nos dice que en lo que se refiere a datos personales

por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tiene derecho a tener una copia. También prevé el derecho de transmisión de datos personales, cuando los mismos hayan facilitad por medio de un contrato. El Sistema Nacional puede crear lineamientos de los parámetros a considerar para determinar un formato estructurado y comúnmente utilizado.

CAPÍTULO I
DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

EJERCICIO DE DERECHOS ARCO

Artículo 43. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

DERECHO DE ACCESO A DATOS PERSONALES

Artículo 44. El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

DERECHO A RECTIFICACIÓN O CORRECCIÓN DE DATOS

Artículo 45. El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados **(supuestos)**.

DERECHO DE CANCELACIÓN DE DATOS

Artículo 46. El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

DERECHO DE OPOSICIÓN. SUPUESTOS

Artículo 47. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

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

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

CAPÍTULO II
DEL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

RECEPCIÓN Y TRÁMITE DE SOLICITUD DE EJERCICIO DE DERECHOS ARCO

Artículo 48. La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a los responsables, se sujetará al procedimiento establecido en el presente Título y demás disposiciones que resulten aplicables en la materia.

REQUISITOS PARA EL EJERCICIO

Artículo 49. Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante.

EJERCICIO DE DERECHOS ARCO POR PERSONA DISTINTA AL TITULAR

El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

EJERCICIO DE DERECHOS ARCO EN MENORES DE EDAD

En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

DATOS PERSONALES DE PERSONAS FALLECIDAS

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente Capítulo, siempre que el titular de los

derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.

EL EJERCICIO DE LOS DERECHOS ARCO ES GRATUITO

Artículo 50. El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable **(costos de reproducción, certificación y envío)**.

DETERMINACIÓN DE COSTOS

Para efectos de acceso a datos personales, las leyes que establezcan los costos de reproducción y certificación deberán considerar en su determinación que los montos permitan o faciliten el ejercicio de este derecho.

CASOS DE ENTREGA SIN COSTO

Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a éste.

CASOS DE ENTREGA SIN COSTO (CONT.)

La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.

PROHIBICIÓN DE COSTO AL TITULAR POR SERVICIO O MEDIO DE PRESENTACIÓN DE LA SOLICITUD

El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular.

SENCILLEZ EN PROCEDIMIENTO DE DERECHOS ARCO

Artículo 51. El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud **(plazo)**.

AMPLIACIÓN DEL PLAZO

El plazo referido en el párrafo anterior 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.

PLAZO DE EJECUCIÓN DE LA RESOLUCIÓN

En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular.

REQUISITOS PARA LA SOLICITUD

Artículo 52. En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:

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

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

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

IV. Descripción clara y precisa de los datos personales: 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. Descripción del derecho ARCO: La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y

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

MODALIDAD EN CASO DE SOLICITUD DE ACCESO

Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

PROCEDIMIENTO EN CASO DE OMISIONES Y DEFECTOS EN LA SOLICITUD

En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere este artículo, y el Instituto o los organismos garantes no cuenten con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio 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 al de la notificación.

PROCEDIMIENTO EN CASO DE OMISIONES Y DEFECTOS EN LA SOLICITUD (CONT.)

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO.

EFECTOS DE LA PREVENCIÓN

La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto, o en su caso, los organismos garantes, para resolver la solicitud de ejercicio de los derechos ARCO.

REQUERIMIENTO POR CANCELACIÓN

Con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable.

REQUERIMIENTO POR OPOSICIÓN

En el caso de la solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

PRESENTACIÓN DE LA SOLICITUD

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable **(receptor)**, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias **(forma de solicitud)**.

TRÁMITE DE LA SOLICITUD

El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibo que corresponda.

MÉTODOS SIMPLIFICADOS PARA EL EJERCICIO DE DERECHOS ARCO

El Instituto y los Organismos garantes, según corresponda, podrán establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.

CARACTERÍSTICAS DE LOS MEDIOS Y PROCEDIMIENTOS RELATIVOS A DERECHOS ARCO

Los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable.

INCOMPETENCIA

Artículo 53. 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 caso de poderlo determinar, orientarlo hacia el responsable competente.

DECLARACIÓN DE INEXISTENCIA DE DATOS PERSONALES

En caso de que el responsable declare inexistencia de los datos personales en sus archivos, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales.

SOLICITUD POR DERECHO DIFERENTE AL ARCO

En caso de que el responsable advierta que la solicitud para el ejercicio de los derechos ARCO corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento al titular.

CASOS EN QUE EXISTA UN TRÁMITE O PROCEDIMIENTO ESPECÍFICO PARA SOLICITAR EL EJERCICIO DE LOS DERECHOS ARCO

Artículo 54. Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los 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, a efecto de que este último decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado para la atención de solicitudes para el ejercicio de los derechos ARCO conforme a las disposiciones establecidas en este Capítulo.

CAUSALES DE IMPROCEDENCIA DE DERECHOS ARCO

Artículo 55. Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:

I. Falta de acreditación: Cuando el titular o su representante no estén debidamente acreditados para ello;

II. Datos que no estén en posesión del responsable: Cuando los datos personales no se encuentren en posesión del responsable;

III. Impedimento: Cuando exista un impedimento legal;

IV. Lesión a derechos de terceros: Cuando se lesionen los derechos de un tercero;

V. Obstáculos a la justicia o a la administración: Cuando se obstaculicen actuaciones judiciales o administrativas;

VI. Restricción por resolución de autoridad competente: 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. Cancelación u oposición ya ejercida: Cuando la cancelación u oposición haya sido previamente realizada;

VIII. Incompetencia: Cuando el responsable no sea competente;

IX. Protección de un interés jurídicamente tutelado: Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;

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

XI. Para mantener la integridad, estabilidad y permanencia del Estado mexicano: 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. Cumplimiento a regulación y supervisión financiera: 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.

FUNDAMENTACIÓN Y MOTIVACIÓN DE LA IMPROCEDENCIA

En todos los casos anteriores, el responsable deberá informar al titular el motivo de su determinación, en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 51 de la presente Ley y demás disposiciones aplicables, y por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.

VÍA PROCEDENTE PARA IMPUGNAR LA NEGATIVA

Artículo 56. Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 94 de la presente Ley.

CAPÍTULO III
DE LA PORTABILIDAD DE LOS DATOS

DERECHO A COPIA DE DATOS PERSONALES EN FORMATOS ELECTRÓNICOS

Artículo 57. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

DERECHO DE TRANSMISIÓN DE DATOS PERSONALES

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

LINEAMIENTOS DE LOS PARÁMETROS A CONSIDERAR PARA DETERMINAR UN FORMATO ESTRUCTURADO Y COMÚNMENTE UTILIZADO

El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

TÍTULO CUARTO
RELACIÓN DEL RESPONSABLE Y ENCARGADO

En este título, se ve la relación que existe entre el responsable—sujeto obligado por esta ley y encargado de dar tratamiento a los datos personales que obtenga—y el encargado—la persona física o moral pública o privada (es decir, una persona, una compañía o incluso un órgano de gobierno) que no es responsable, pero que trata datos personales a nombre y cuenta de este.

El artículo 58 señala las facultades del encargado de datos personales, consistentes en el tratamiento exclusivo de los datos personales, sin poder tomar decisión alguna que afecte el alcance y contenido de esta actividad.

En el numeral 59. se establece que la relación entre encargado y responsable debe ser formalizada (puesta por escrito y por medio de un instrumento que prevea la Ley), por lo general, a través de un contrato, y éste debe contener las siguientes cláusulas generales relacionadas con los servicios que preste el encargado: realizar el tratamiento de los datos personales conforme a lo instruido por el responsable, abstenerse de tratar los datos personales para finalidades distintas a las instruidas, implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables, informar al responsable cuando ocurra una vulneración a los datos personales, guardar confidencialidad respecto de los datos personales tratados; suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, abstenerse de transferir los datos personales salvo que el responsable así lo determine

Los contratos tienen como límites las disposiciones de la Ley y si el encargado incumple con sus obligaciones, éste asumirá el carácter de responsable conforme a la legislación aplicable (artículo 60). El encargado puede también subcontratar (por medio de un contrato) servicios de tratamiento de datos personales por cuenta del responsable siempre y cuando esté su autorización expresa. El subcontratado se asume como encargado (artículos 61 y 62).

El artículo 63 regula el cómputo en la nube para tratamiento de datos personales, es decir, que el responsable pueda contratar un servicio para tratar datos personales por medio de una infraestructura de red. La Ley establece los siguientes criterios para la contratación de cómputo en nube (artículo 64):

Requerimientos mínimos:

- Que sea afín a los principios y derechos de Ley.
- Que transparente las subcontrataciones.
- Que no incluya cláusulas que lo hagan propietario o titular de la información.
- Que sea confidencial.

Mecanismos mínimos:

- Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
- Permitir al responsable limitar el tipo de tratamiento de los datos personales.
- Establecer y mantener medidas de seguridad para la protección de los datos personales.
- Garantizar la supresión de los datos personales.
- Impedir el acceso a los datos a personas que no cuenten con privilegios de acceso.

CAPÍTULO ÚNICO
RESPONSABLE Y ENCARGADO

FACULTADES DEL ENCARGADO DE DATOS PERSONALES

Artículo 58. El encargado deberá realizar las actividades de tratamiento de los 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.

FORMALIZACIÓN DE LA RELACIÓN ENTRE RESPONSABLE Y ENCARGADO

Artículo 59. La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

CONTENIDO DEL CONTRATO

En el contrato o instrumento jurídico que decida el responsable se deberán prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

I. Realizar el tratamiento de los datos personales conforme a lo instruido por el responsable: 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: 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: Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;

IV. Informar al responsable cuando ocurra una vulneración a los datos personales: 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: 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: 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 que el responsable así lo determine: 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.

LÍMITES AL CONTRATO

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la presente Ley y demás disposiciones aplicables, así como lo establecido en el aviso de privacidad correspondiente.

INCUMPLIMIENTO DEL CONTRATO. RESPONSABILIDAD SUBSIDIARIA

Artículo 60. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.

SUBCONTRATACIÓN

Artículo 61. El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie la autorización expresa de este último. El subcontratado asumirá el carácter de encargado en los términos de la presente la Ley y demás disposiciones que resulten aplicables en la materia **(carácter del subcontratado)**.

OTORGAMIENTO DE FACULTAD DE SUBCONTRATAR EN EL CONTRATO

Cuando el contrato o el instrumento jurídico mediante el cual se haya formalizado la relación entre el responsable y el encargado, prevea que este último pueda llevar a

cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el párrafo anterior se entenderá como otorgada a través de lo estipulado en éstos.

FORMALIZACIÓN DE LA SUBCONTRATACIÓN

Artículo 62. Una vez obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que decida, de conformidad con la normatividad que le resulte aplicable, y permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en el presente Capítulo.

CÓMPUTO EN LA NUBE PARA TRATAMIENTO DE DATOS PERSONALES

Artículo 63. El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

CRITERIOS PARA LA CONTRATACIÓN DE CÓMPUTO EN NUBE

Artículo 64. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Requerimientos mínimos: Cumpla, al menos, con lo siguiente:

a) Sea afín a los principios y derechos de Ley: Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;

b) Transparente las subcontrataciones: Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;

c) No incluya cláusulas que lo hagan propietario o titular de la información: Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y

d) Sea confidencial: Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio;

II. Mecanismos mínimos: Cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta: Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;

b) Permitir al responsable limitar el tipo de tratamiento de los datos personales: Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

c) Establecer y mantener medidas de seguridad para la protección de los datos personales: Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;

d) Garantizar la supresión de los datos personales: Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, y

e) Impedir el acceso a los datos a personas que no cuenten con privilegios de acceso: Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la presente Ley y demás disposiciones que resulten aplicables en la materia.

TÍTULO QUINTO
COMUNICACIONES DE DATOS PERSONALES

CAPÍTULO V
DEL CONSEJO CONSULTIVO DE LOS ORGANISMOS GARANTES

En este título, se hablan de las transferencias y remisiones de datos personales. Las primeras deben entenderse como el movimiento de datos personales de un responsable a una persona distinta del titular, responsable o encargado; las segundas son el movimiento de datos personales entre un responsable y un encargado.

El artículo 65 nos dice que toda transferencia debe tener el consentimiento del titular y en el 66 se establece que dentro del contrato firmado inicialmente con el mismo puede ponerse una cláusula que contemple el consentimiento de transferencias; es decir, no se necesita un nuevo contrato. En este artículo, también se establece cómo las transferencias nacionales hechas entre responsables por virtud de un mandato de Ley no deben formalizarse por contrato, al igual que las internacionales, que se hagan por virtud de un tratado o ley y sean a petición de autoridad extranjera u organismo internacional competente.

El requerimiento principal para la transferencia nacional de datos personales es que el receptor los trate para la finalidad a la que fueron transferidos, guardando confidencialidad (artículo 67). Las transferencias internacionales, sólo se pueden realizar cuando se obligue al receptor a proteger los datos personales en los términos de la ley mexicana (artículo 68). Toda transferencia debe llevar un aviso de privacidad donde se le señale al receptor la forma en que se tratan los datos personales (artículo 69).

El artículo 70 señala los casos de excepción al consentimiento en la transferencia: la existencia de ley o tratado internacional que lo prevea, que se realicen transferencias entre responsables para el ejercicio de facultades compatibles con la finalidad con la que se obtuvieron los datos, para la persecución de delitos, para el reconocimiento, ejercicio o defensa de un derecho, para la prevención, diagnóstico o tratamiento médico y la prestación de asistencia sanitaria, para el mantenimiento o cumplimiento de una relación jurídica entre responsable y titular, por virtud de un contrato celebrado por el responsable y un tercero, para los casos en los que el

responsable no esté obligado a recabar el consentimiento del titular de datos personales y cuando la transferencia sea necesaria por razones de seguridad nacional.

El artículo 71 establece que las remisiones de datos no requieren ser informadas al titular, ni contar con su consentimiento. Es decir, si un responsable subcontrata a una compañía para tratar datos personales en su nombre, el movimiento de datos que haga no requiere ser comunicado ni consentido por los titulares de los datos personales.

CAPÍTULO ÚNICO
DE LAS TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES

EL CONSENTIMIENTO EN LAS TRANSFERENCIAS DE DATOS PERSONALES

Artículo 65. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de esta Ley.

FORMALIZACIÓN DE LAS TRANSFERENCIAS

Artículo 66. 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 responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

CASOS DE EXCEPCIÓN

Lo dispuesto en el párrafo anterior, no será aplicable en los siguientes casos:

I. En transferencias nacionales: Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o

II. En transferencias internacionales: Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

REQUERIMIENTOS PARA LA TRANSFERENCIA NACIONAL DE DATOS PERSONALES

Artículo 67. Cuando la transferencia sea 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.

REQUERIMIENTOS PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Artículo 68. El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.

AVISO DE PRIVACIDAD

Artículo 69. En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular.

CASOS DE EXCEPCIÓN AL CONSENTIMIENTO EN LA TRANSFERENCIA

Artículo 70. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:

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

II. Transferencias entre responsables: 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. Para la persecución de delitos: Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;

IV. Para el reconocimiento, ejercicio o defensa de un derecho: 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. Para la prevención, diagnóstico o tratamiento médico y la prestación de asistencia sanitaria: 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. Para el mantenimiento o cumplimiento de una relación jurídica entre responsable y titular: Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;

VII. Por virtud de un contrato celebrado por el responsable y un tercero: 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. Artículo 22: 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. Seguridad nacional: Cuando la transferencia sea necesaria por razones de seguridad nacional.

La actualización de algunas de las excepciones previstas en este artículo, no exime al responsable de cumplir con las obligaciones previstas en el presente Capítulo que resulten aplicables.

REMISIONES DE DATOS ENTRE RESPONSABLE Y ENCARGADO

Artículo 71. Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.

TÍTULO SEXTO
ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

En este título, se habla de “acciones preventivas,” es decir, de medidas que uno puede tomar para llevar a cabo las condiciones necesarias para que la vulneración de datos personales sea lo más difícil posible. El primer capítulo versa de los esquemas de mejores prácticas, los cuales buscan mejorar el funcionamiento de los sistemas de resguardo de datos personales; el segundo versa sobre las bases de datos que poseen organismos de seguridad y de procuración y administración de justicia (ministerio público, policía y jueces).

Los esquemas de mejores prácticas son una serie de destrezas que un responsable de datos personales puede realizar con los siguientes objetivos: elevar el nivel de protección, armonizar el tratamiento de datos personales, facilitar el ejercicio de los derechos ARCO, facilitar las transferencias de datos personales, complementar las disposiciones previstas en la normatividad y demostrar el cumplimiento de la normatividad aplicable (artículo 72). Todo esquema de mejores prácticas debe cumplir con dos requisitos: cumplir con los parámetros que emitan el Instituto y los organismos garantes por medio de reglas de operación y ser evaluado, validado y reconocido ante el Instituto. Todo lo que se certifique como mejor práctica debe inscribirse en un registro (artículo 73).

Los responsables que realicen cambios a sus políticas públicas o a su tecnología de resguardo de datos personales deben realizar una evaluación de impacto en la protección de datos personales, treinta días anteriores a la implementación de la medida para que el Sistema Nacional de Transparencia haga una determinación de su contenido (artículos 74 y 77). El INAI o los organismos garantes locales pueden emitir recomendaciones no vinculantes sobre la evaluación de impacto hasta treinta días siguientes a su presentación (artículo 78).

El artículo 75 establece una serie de casos de tratamiento intensivo o relevante de datos: cuando existan riesgos inherentes a los datos personales a tratar, cuando

haya datos personales sensibles, cuando haya transferencias de datos. El 76 establece criterios adicionales para el tratamiento intensivo: el Sistema Nacional de Transparencia tiene la facultad de emitir, en función de: el número de titulares, el público objetivo, el desarrollo de la tecnología utilizada y la relevancia del tratamiento de datos personales en atención a su impacto.

En lo que respecta a las instancias de seguridad, procuración y administración de Justicia, el artículo 80 establece los parámetros de la obtención, tratamiento y almacenaje de datos personales, además de las obligaciones de las autoridades que los almacenen. En el artículo 81, se establece que deben aplicarse los principios establecidos en el Título Segundo de la Ley para el tratamiento de datos personales y su almacenamiento, además de la inviolabilidad de las comunicaciones privadas.

Por último, en el artículo 82 se establece que los responsables de datos personales en materia de seguridad, procuración y administración de Justicia deben implementar medidas de seguridad para garantizar la integridad, disponibilidad y confidencialidad de la información.

CAPÍTULO I
DE LAS MEJORES PRÁCTICAS

ESQUEMAS DE MEJORES PRÁCTICAS. SUJETO QUE LAS PUEDE DESARROLLAR

Artículo 72. Para el cumplimiento de las obligaciones previstas en la presente Ley, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto:

I. Elevar el nivel de protección: Elevar el nivel de protección de los datos personales;

II. Armonizar el tratamiento de datos personales: Armonizar el tratamiento de datos personales en un sector específico;

III. Facilitar el ejercicio de los derechos ARCO: Facilitar el ejercicio de los derechos ARCO por parte de los titulares;

IV. Facilitar las transferencias de datos personales: Facilitar las transferencias de datos personales;

V. Complementar las disposiciones previstas en la normatividad: Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y

VI. Demostrar el cumplimiento de la normatividad aplicable: Demostrar ante el Instituto o, en su caso, los Organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

REQUERIMIENTO DE LOS ESQUEMAS DE MEJORES PRÁCTICAS

Artículo 73. Todo esquema de mejores prácticas que busque la validación o reconocimiento por parte del Instituto o, en su caso, de los Organismos garantes deberá:

I. Cumplir con los parámetros que emitan el Instituto y los organismos garantes: Cumplir con los parámetros que para tal efecto emitan, según corresponda, el Instituto y los Organismos garantes conforme a los criterios que fije el primero, y

II. Ser evaluado, validado y reconocido ante el Instituto: Ser notificado ante el Instituto o, en su caso, los Organismos garantes de conformidad con el procedimiento establecido en los parámetros señalados en la fracción anterior, a fin de que sean evaluados y, en su caso, validados o reconocidos e inscritos en el registro al que refiere el último párrafo de este artículo.

REGLAS DE OPERACIÓN DE LOS REGISTROS

El Instituto y los Organismos garantes, según corresponda, deberán emitir las reglas de operación de los registros en los que se inscribirán aquellos esquemas de mejores prácticas validados o reconocidos. Los Organismos garantes, podrán inscribir los esquemas de mejores prácticas que hayan reconocido o validado en el registro administrado por el Instituto, de acuerdo con las reglas que fije este último **(inscripción de los esquemas de mejores prácticas)**.

EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

Artículo 74. Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los Organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

El contenido de la evaluación de impacto a la protección de datos personales deberá determinarse por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales **(determinación del contenido de la evaluación de impacto)**.

CASOS DE TRATAMIENTO INTENSIVO O RELEVANTE DE DATOS

Artículo 75. Para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

I. Riesgos inherentes: Existan riesgos inherentes a los datos personales a tratar;

II. Datos personales sensibles: Se traten datos personales sensibles, y

III. Transferencias de datos: Se efectúen o pretendan efectuar transferencias de datos personales.

CRITERIOS ADICIONALES PARA EL TRATAMIENTO INTENSIVO

Artículo 76. El Sistema Nacional podrá emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales, de conformidad con lo dispuesto en el artículo anterior, en función de:

I. Número de titulares: El número de titulares;

II. Público objetivo: El público objetivo;

III. Desarrollo de la tecnología utilizada: El desarrollo de la tecnología utilizada, y

IV. Relevancia del tratamiento de datos personales en atención a su impacto: La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue.

EVALUACIÓN

Artículo 77. Los sujetos obligados que realicen una Evaluación de impacto en la protección de datos personales **(receptores)**, deberán presentarla ante el Instituto o los Organismos garantes, según corresponda, treinta días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología **(plazo y casos)**, ante el Instituto o los organismos garantes, según corresponda, a efecto de que emitan las recomendaciones no vinculantes correspondientes **(evaluadores y recomendaciones)**.

RECOMENDACIONES NO VINCULANTES SOBRE LA EVALUACIÓN DE IMPACTO

Artículo 78. El Instituto y los Organismos garantes, según corresponda, deberán emitir, de ser el caso, recomendaciones no vinculantes sobre la Evaluación de impacto en la protección de datos personales presentado por el responsable.

PLAZO

El plazo para la emisión de las recomendaciones a que se refiere el párrafo anterior será dentro de los treinta días siguientes contados a partir del día siguiente a la presentación de la evaluación.

EXCEPCIONES A LA EVALUACIÓN DE IMPACTO

Artículo 79. Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la Evaluación de impacto en la protección de datos personales.

CAPÍTULO II

DE LAS BASES DE DATOS EN POSESIÓN DE INSTANCIAS DE SEGURIDAD, PROCURACIÓN Y ADMINISTRACIÓN DE JUSTICIA

PARÁMETROS DE LOS DATOS PERSONALES

Artículo 80. La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de las sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto **(almacenamiento)**.

OBLIGACIONES DE LAS AUTORIDADES QUE ALMACENEN DATOS PERSONALES

Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.

PRINCIPIOS RECTORES DEL TRATAMIENTO DE DATOS PERSONALES Y SU ALMACENAMIENTO

Artículo 81. En el tratamiento de datos personales así como en el uso de las bases de datos para su almacenamiento, que realicen los sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los principios establecidos en el Título Segundo de la presente Ley.

INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS

Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio

Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.

CALIDAD DEL ALMACENAMIENTO DE DATOS PERSONALES

Artículo 82. Los responsables de las bases de datos a que se refiere este Capítulo, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado **(propósito)**.

TÍTULO SÉPTIMO
RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS

Todo responsable del resguardo de datos personales debe contar con un Comité y una Unidad de Transparencia para el manejo de datos personales. Todo responsable de datos también es sujeto obligado de transparencia, pues la Ley General de Transparencia y Acceso a la Información Pública es en muchos casos subsidiaria a la legislación de datos personales. El Comité es la autoridad máxima en materia de protección de datos personales y tiene las siguientes facultades: garantizar el derecho de protección de los datos personales, instituir procedimientos internos sobre derechos ARCO, resolver determinaciones sobre inexistencia de datos personales o negativa de ejercicio de derechos ARCO, establecer y supervisar criterios, supervisar el contenido de documentos de seguridad, seguir y cumplir con las resoluciones del Instituto, capacitar y actualizar a servidores públicos en la materia, vista al órgano interno de control sobre irregularidades.

La Unidad de Transparencia tiene las siguientes funciones: auxiliar y orientar al titular que lo requiera, gestionar las solicitudes para el ejercicio de los derechos ARCO, establecer mecanismos para la correcta gestión de datos personales, informar al titular de los montos a cubrir por la reproducción y envío de datos personales, proponer los procedimientos internos para la gestión de solicitudes, aplicar evaluación de calidad de la gestión de los solicitantes, asesorar en la materia al responsable. Esta unidad puede designar un oficial de protección de datos personales para realizar las funciones antes mencionadas.

Asimismo, el responsable debe buscar el mayor acceso posible para discapacitados y grupos vulnerables para que puedan ejercer sus derechos ARCO en igualdad de condiciones. Para ello, se pueden celebrar acuerdos con instituciones públicas para accesibilidad.

CAPÍTULO I
COMITÉ DE TRANSPARENCIA

COMITÉ DE TRANSPARENCIA

Artículo 83. Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

RANGO

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales.

FACULTADES DEL COMITÉ DE TRANSPARENCIA EN MATERIA DE DATOS PERSONALES

Artículo 84. Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:

I. Garantizar el derecho de protección de los datos personales: Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

II. Instituir procedimientos internos sobre derechos ARCO: Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

III. Resolver determinaciones sobre inexistencia de datos personales o negativa de ejercicio de derechos ARCO: Confirmar, modificar o revocar las

determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;

IV. Establecer y supervisar criterios: Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;

V. Supervisar el contenido de documentos de seguridad: Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

VI. Seguir y cumplir con las resoluciones del Instituto: Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;

VII. Capacitar y actualizar a servidores públicos en la materia: Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

VIII. Vista al órgano interno de control sobre irregularidades: Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

CAPÍTULO II
DE LA UNIDAD DE TRANSPARENCIA

UNIDAD DE TRANSPARENCIA

Artículo 85. Cada responsable contará con una Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, esta Ley y demás normativa aplicable, que tendrá las siguientes funciones **(facultades)**:

I. Auxiliar y orientar al titular que lo requiera: Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;

II. Gestionar las solicitudes para el ejercicio de los derechos ARCO: Gestionar las solicitudes para el ejercicio de los derechos ARCO;

III. Establecer mecanismos para la correcta gestión de datos personales: Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;

IV. Informar al titular de los montos a cubrir por la reproducción y envío de datos personales: Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;

V. Proponer los procedimientos internos para la gestión de solicitudes: Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

VI. Aplicar evaluación de calidad de la gestión de los solicitantes: Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y

VII. Asesorar en la materia: Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia **(casos de designación)**, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia **(funciones)**.

ACUERDOS CON INSTITUCIONES PÚBLICAS PARA ACCESIBILIDAD

Los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

IGUALDAD EN EL EJERCICIO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Artículo 86. El responsable procurará que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.

DESIGNACIÓN DEL TITULAR DE LA UNIDAD DE TRANSPARENCIA

Artículo 87. En la designación del titular de la Unidad de Transparencia, el responsable estará a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

TÍTULO OCTAVO
ORGANISMOS GARANTES

En lo que se refiere a los órganos gubernamentales encargados de asegurar la protección de datos personales, a nivel federal se encuentra el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y a nivel local, los diversos órganos garantes. Fuera del desarrollo que hace de los mismos la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y la legislación local en materia de transparencia, este título desarrolla las facultades que tienen en materia de datos personales

El artículo 89 establece las facultades del Instituto Nacional de Transparencia: garantizar el ejercicio del derecho a la protección de datos personales, interpretar la Ley en el ámbito administrativo, conocer y resolver los recursos de revisión, atraer recursos de revisión de interés y trascendencia, conocer y resolver recursos de inconformidad, conocer, sustanciar y resolver procedimientos de verificación; establecer y ejecutar las medidas de apremio, denunciar presuntas infracciones, coordinarse con las autoridades para dar accesibilidad en lenguas indígenas, garantizar condiciones de accesibilidad para grupos vulnerables, elaborar y publicar estudios e investigaciones, proporcionar apoyo técnico a los responsables, emitir recomendaciones, estándares y mejores prácticas; vigilar y verificar el cumplimiento de las disposiciones de Ley, administrar el registro de esquemas de mejores prácticas, emitir las recomendaciones no vinculantes correspondientes a la evaluación de impacto, emitir disposiciones generales para el desarrollo del procedimiento de verificación, realizar las evaluaciones correspondientes a los esquemas de mejores prácticas que sean notificados; emitir disposiciones administrativas para el cumplimiento de principios, deberes y obligaciones de la Ley, celebrar convenio para homologación del tratamiento de datos personales en sectores específicos, definir y desarrollar el sistema de certificación en materia de protección de datos personales, presidir el Sistema Nacional de Transparencia, celebrar convenios con organizaciones garantes; promover el conocimiento del

derecho de la protección de datos personales, diseñar y aplicar indicadores y criterios para evaluar el desempeño de los responsables, promover la capacitación y actualización en materia de protección de datos personales, emitir lineamientos generales para el debido tratamiento de datos personales; emitir lineamientos para homologar el ejercicio de los derechos ARCO, emitir lineamientos para homologar el ejercicio de los derechos ARCO, cooperar con otras autoridades y organismos nacionales e internacionales, promover el ejercicio y tutela del derecho de protección de datos por medio de la Plataforma Nacional, interponer acciones de inconstitucionalidad, interponer controversias constitucionales; cooperar con otras autoridades nacionales o internacionales para combatir el indebido tratamiento de datos personales, diseñar, vigilar y operar el sistema de buenas prácticas, celebrar convenios con organismos garantes y responsables y otras que confiera la legislación aplicable.

En el artículo 91, se establecen las facultades de los organismos garantes locales en materia de datos personales: conocer, sustanciar y resolver recursos de revisión, formular petición al INAI para atraer recursos de revisión, imponer medidas de apremio, promover y difundir el ejercicio del derecho a la protección de datos personales; coordinarse con autoridades para lograr accesibilidad de lenguas indígenas, garantizar accesibilidad a grupos vulnerables, elaborar y publicar estudios e investigaciones, dar a conocer presuntas responsabilidades por incumplimiento a la Ley, proporcionar al Instituto los elementos que requiera para resolver los recursos de inconformidad; suscribir convenios de colaboración con el Instituto, vigilar el cumplimiento de la Ley, promover el conocimiento del derecho a la protección de datos personales, aplicar indicadores y criterios para evaluar el desempeño de los responsables, promover la capacitación del derecho a la protección de datos personales; solicitar la cooperación del Instituto, administrar la Plataforma Nacional de Transparencia, interponer acciones de inconstitucionalidad, emitir recomendaciones no vinculantes respecto a la evaluación de impacto.

En el artículo 92, se establece el deber de los responsables de colaborar con el Instituto y los garantes locales para la capacitación y actualización permanente de servidores públicos en materia de datos personales. En el numeral 93, se establecen las obligaciones de coordinación y promoción de derechos de datos personales que tienen el instituto y los organismos garantes, que en específico deben realizar tres cosas: promover la inclusión de derecho de datos personales en materia educativa, impulsar la integración de centros de investigación, difusión y docencia, fomentar la creación de espacios de participación social y ciudadana.

CAPÍTULO I

DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

INSTITUTO NACIONAL DE TRANSPARENCIA Y CONSEJO CONSULTIVO

Artículo 88. En la integración, procedimiento de designación y funcionamiento del Instituto y del Consejo Consultivo se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

ATRIBUCIONES DEL INAI EN MATERIA DE DATOS PERSONALES

Artículo 89. Además de las facultades que le son conferidas en la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normatividad que le resulte aplicable, el Instituto tendrá las siguientes atribuciones:

I. Garantizar el ejercicio del derecho a la protección de datos personales: Garantizar el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados;

II. Interpretar la Ley: Interpretar la presente Ley en el ámbito administrativo;

III. Conocer y resolver los recursos de revisión: Conocer y resolver los recursos de revisión que interpongan los titulares, en términos de lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;

IV. Atraer recursos de revisión de interés y trascendencia: Conocer y resolver, de oficio o a petición fundada por los organismos garantes, los recursos de revisión que por su interés y trascendencia así lo ameriten, en términos de lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;

V. Conocer y resolver recursos de inconformidad: Conocer y resolver los recursos de inconformidad que interpongan los titulares, en contra de las resoluciones

emitidas por los organismos garantes, de conformidad con lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;

VI. Conocer, sustanciar y resolver procedimientos de verificación: Conocer, sustanciar y resolver los procedimientos de verificación;

VII. Establecer y ejecutar las medidas de apremio: Establecer y ejecutar las medidas de apremio previstas en términos de lo dispuesto por la presente Ley y demás disposiciones que resulten aplicables en la materia;

VIII. Denunciar presuntas infracciones: Denunciar ante las autoridades competentes las presuntas infracciones a la presente Ley y, en su caso, aportar las pruebas con las que cuente;

IX. Coordinarse con las autoridades para dar accesibilidad en lenguas indígenas: Coordinarse con las autoridades competentes para que las solicitudes para el ejercicio de los derechos ARCO y los recursos de revisión que se presenten en lengua indígena, sean atendidos en la misma lengua;

X. Garantizar condiciones de accesibilidad para grupos vulnerables: Garantizar, en el ámbito de su respectiva competencia, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales;

XI. Elaborar y publicar estudios e investigaciones: Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de la presente Ley;

XII. Proporcionar apoyo técnico a los responsables: Proporcionar apoyo técnico a los responsables para el cumplimiento de las obligaciones establecidas en la presente Ley;

XIII. Emitir recomendaciones, estándares y mejores prácticas: Divulgar y emitir recomendaciones, estándares y mejores prácticas en las materias reguladas por la presente Ley;

XIV. Vigilar y verificar el cumplimiento de las disposiciones de Ley: Vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley;

XV. Administrar el registro de esquemas de mejores prácticas: Administrar el registro de esquemas de mejores prácticas a que se refiere la presente Ley y emitir sus reglas de operación;

XVI. Emitir las recomendaciones no vinculantes correspondientes a la evaluación de impacto: Emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de impacto en la protección de datos personales que le sean presentadas;

XVII. Emitir disposiciones generales para el desarrollo del procedimiento de verificación: Emitir disposiciones generales para el desarrollo del procedimiento de verificación;

XVIII. Realizar las evaluaciones correspondientes a los esquemas de mejores prácticas que sean notificados: Realizar las evaluaciones correspondientes a los esquemas de mejores prácticas que les sean notificados, a fin de resolver sobre la procedencia de su reconocimiento o validación e inscripción en el registro de esquemas de mejores prácticas, así como promover la adopción de los mismos;

XIX. Emitir disposiciones administrativas para el cumplimiento de principios, deberes y obligaciones de la Ley: Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general para el debido cumplimiento de los principios, deberes y obligaciones que establece la presente Ley, así como para el ejercicio de los derechos de los titulares;

XX. Celebrar convenio para homologación del tratamiento de datos personales en sectores específicos: Celebrar convenios con los responsables para desarrollar programas que tengan por objeto homologar tratamientos de datos personales en sectores específicos, elevar la protección de los datos personales y realizar cualquier mejora a las prácticas en la materia;

XXI. Definir y desarrollar el sistema de certificación en materia de protección de datos personales: Definir y desarrollar el sistema de certificación en materia de protección de datos personales, de conformidad con lo que se establezca en los parámetros a que se refiere la presente Ley;

XXII. Presidir el Sistema Nacional: Presidir el Sistema Nacional a que se refiere el artículo 10 de la presente Ley;

XXIII. Celebrar convenios con organizaciones garantes: Celebrar convenios con los organismos garantes que coadyuven al cumplimiento de los objetivos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;

XXIV. Promover el conocimiento del derecho de la protección de datos personales: Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales, así como de sus prerrogativas;

XXV. Diseñar y aplicar indicadores y criterios para evaluar el desempeño de los responsables: Diseñar y aplicar indicadores y criterios para evaluar el desempeño de los responsables respecto al cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia;

XXVI. Promover la capacitación y actualización en materia de protección de datos personales: Promover la capacitación y actualización en materia de protección de datos personales entre los responsables;

XXVII. Emitir lineamientos generales para el debido tratamiento de datos personales: Emitir lineamientos generales para el debido tratamiento de los datos personales;

XXVIII. Emitir lineamientos para homologar el ejercicio de los derechos ARCO: Emitir lineamientos para homologar el ejercicio de los derechos ARCO;

XXIX. Emitir lineamientos para homologar el ejercicio de los derechos ARCO: Emitir criterios generales de interpretación para garantizar el derecho a la protección de datos personales;

XXX. Cooperar con otras autoridades y organismos nacionales e internacionales: Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos personales, de conformidad con las disposiciones previstas en la presente Ley y demás normativa aplicable;

XXXI. Promover el ejercicio y tutela del derecho de protección de datos por medio de la Plataforma Nacional: Promover e impulsar el ejercicio y tutela del derecho a la protección de datos personales a través de la implementación y administración de la Plataforma Nacional, a que se refiere la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable;

XXXII. Interponer acciones de inconstitucionalidad: Interponer, cuando así lo aprueben la mayoría de sus Comisionados, acciones de inconstitucionalidad en contra de leyes de carácter federal o estatal, así como de los Tratados Internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho a la protección de datos personales;

XXXIII. Interponer controversias constitucionales: Promover, cuando así lo aprueben la mayoría de sus Comisionados, las controversias constitucionales en términos del artículo 105, fracción I, inciso l), de la Constitución Política de los Estados Unidos Mexicanos;

XXXIV. Cooperar con otras autoridades nacionales o internacionales para combatir el indebido tratamiento de datos personales: Cooperar con otras autoridades nacionales o internacionales para combatir conductas relacionadas con el indebido tratamiento de datos personales;

XXXV. Diseñar, vigilar y operar el sistema de buenas prácticas: Diseñar, vigilar y, en su caso, operar el sistema de buenas prácticas en materia de protección de datos personales, así como el sistema de certificación en la materia, a través de normativa que el Instituto emita para tales fines;

XXXVI. Celebrar convenios con organismos garantes y responsables: Celebrar convenios con los organismos garantes y responsables que coadyuven al cumplimiento de los objetivos previstos en la presente Ley y demás disposiciones que

resulten aplicables en la materia, y

XXXVII. Cláusula residual: Las demás que le confiera la presente Ley y demás ordenamientos aplicables.

CAPÍTULO II
DE LOS ORGANISMOS GARANTES

ORGANISMOS GARANTES

Artículo 90. En la integración, procedimiento de designación y funcionamiento de los organismos garantes se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

FACULTADES PARA LOS ORGANISMOS GARANTES EN MATERIA DE DATOS PERSONALES

Artículo 91. Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que les sean conferidas en la normatividad que les resulte aplicable, los organismos garantes tendrán las siguientes atribuciones:

I. Conocer, sustanciar y resolver recursos de revisión: Conocer, sustanciar y resolver, en el ámbito de sus respectivas competencias, de los recursos de revisión interpuestos por los titulares, en términos de lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;

II. Formular petición al INAI para que atraiga recursos de revisión: Presentar petición fundada al Instituto, para que conozca de los recursos de revisión que por su interés y trascendencia así lo ameriten, en términos de lo previsto en la presente Ley y demás disposiciones que resulten aplicables en la materia;

III. Imponer medidas de apremio: Imponer las medidas de apremio para asegurar el cumplimiento de sus resoluciones;

IV. Promover y difundir el ejercicio del derecho a la protección de datos personales: Promover y difundir el ejercicio del derecho a la protección de datos personales;

V. Coordinarse con autoridades para lograr accesibilidad de lenguas indígenas:

Coordinarse con las autoridades competentes para que las solicitudes para el ejercicio de los derechos ARCO y los recursos de revisión que se presenten en lenguas indígenas, sean atendidos en la misma lengua;

VI. Garantizar accesibilidad a grupos vulnerables: Garantizar, en el ámbito de sus respectivas competencias, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales;

VII. Elaborar y publicar estudios e investigaciones: Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de la presente Ley;

VIII. Dar a conocer presuntas responsabilidades por incumplimiento a la Ley: Hacer del conocimiento de las autoridades competentes, la probable responsabilidad derivada del incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones que resulten aplicables;

IX. Proporcionar al Instituto los elementos que requiera para resolver los recursos de inconformidad: Proporcionar al Instituto los elementos que requiera para resolver los recursos de inconformidad que le sean presentados, en términos de lo previsto en el Título Noveno, Capítulo II de la presente Ley y demás disposiciones que resulten aplicables en la materia;

X. Suscribir convenios de colaboración con el Instituto: Suscribir convenios de colaboración con el Instituto para el cumplimiento de los objetivos previstos en la presente Ley y demás disposiciones aplicables;

XI. Vigilar el cumplimiento de la Ley: Vigilar, en el ámbito de sus respectivas competencias, el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia;

XII. Promover el conocimiento del derecho a la protección de datos personales: Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales, así como de sus prerrogativas;

XIII. Aplicar indicadores y criterios para evaluar el desempeño de los responsables: Aplicar indicadores y criterios para evaluar el desempeño de los responsables respecto del cumplimiento de la presente Ley y demás disposiciones que resulten aplicables;

XIV. Promover la capacitación del derecho a la protección de datos personales: Promover la capacitación y actualización en materia de protección de datos personales entre los responsables;

XV. Solicitar la cooperación del Instituto: Solicitar la cooperación del Instituto en los términos del artículo 89, fracción XXX de la presente Ley;

XVI. Administrar la Plataforma Nacional de Transparencia: Administrar, en el ámbito de sus competencias, la Plataforma Nacional de Transparencia;

XVII. Interponer acciones de inconstitucionalidad: Según corresponda, interponer acciones de inconstitucionalidad en contra de leyes expedidas por las legislaturas de las Entidades Federativas, que vulneren el derecho a la protección de datos personales, y

XVIII. Emitir recomendaciones no vinculantes respecto a la evaluación de impacto: Emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de impacto en protección de datos personales que le sean presentadas.

CAPÍTULO III
DE LA COORDINACIÓN Y PROMOCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

COLABORACIÓN PARA LA CAPACITACIÓN Y ACTUALIZACIÓN PERMANENTE DE SERVIDORES PÚBLICOS

Artículo 92. Los responsables deberán colaborar con el Instituto y los organismos garantes, según corresponda, para capacitar y actualizar de forma permanente a todos sus servidores públicos en materia de protección de datos personales, a través de la impartición de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.

OBLIGACIONES DE COORDINACIÓN Y PROMOCIÓN DE DERECHOS DE DATOS PERSONALES

Artículo 93. El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias, deberán:

I. Inclusión de derecho de datos personales en materia educativa: Promover que en los programas y planes de estudio, libros y materiales que se utilicen en las instituciones educativas de todos los niveles y modalidades del Estado, se incluyan contenidos sobre el derecho a la protección de datos personales, así como una cultura sobre el ejercicio y respeto de éste;

II. Impulsar la integración de centros de investigación, difusión y docencia: Impulsar en conjunto con instituciones de educación superior, la integración de centros de investigación, difusión y docencia sobre el derecho a la protección de datos personales que promuevan el conocimiento sobre este tema y coadyuven con el Instituto y los Organismos garantes en sus tareas sustantivas, y

III. Fomentar la creación de espacios de participación social y ciudadana: Fomentar la creación de espacios de participación social y ciudadana que estimulen el intercambio de ideas entre la sociedad, los órganos de representación ciudadana y los responsables.

TÍTULO NOVENO
DE LOS PROCEDIMIENTOS DE IMPUGNACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Este título contiene la información más técnica y jurídica de toda la Ley porque versa sobre las impugnaciones—los instrumentos jurídicos que sirven para invalidar un acto de autoridad ("resolución") con el que no estamos de acuerdo. Este título establece cuáles son las reglas comunes a los instrumentos con los que se cuenta (Capítulo I, Disposiciones Comunes a los Recursos de Revisión y Recursos de Inconformidad) y nos dice cuáles son (Capitulo II Recurso de Revisión; Capítulo III Recurso de Inconformidad) y aspectos particulares como la atracción de recursos, la revisión en materia de seguridad nacional y los criterios de interpretación.

En el artículo 94, se establecen los medios que existen para presentar el recurso de revisión o de inconformidad: el escrito libre, correo certificado, formatos que emita el Instituto y organismos garantes, medios electrónicos y otros medios que establezca el Instituto o los garantes locales. A diferencia de la transparencia, donde no es necesario acreditar la identidad del recurrente, en materia de datos se debe hacer de forma obligatoria y por medio de uno de los siguientes instrumentos: identificación oficial, firma electrónica, mecanismos de autenticación autorizados por el INAI y los garantes locales (artículo 95).

La acreditación del representante si el recurso no se hace a título propio varía si el representante es una persona física o moral. Si es una persona física, se puede acreditar como representante si presenta carta poder simple ante dos testigos, con instrumento público o con declaración en comparecencia personal del titular y del representante ante el Instituto. Si es persona moral, se hace por medio de instrumento público (artículo 96). También proceden los recursos de revisión e inconformidad sobre los datos de una persona fallecida si el que interpone dicho instrumento acredita tener un interés jurídico o legítimo (artículo 97).

En el artículo 98, se establecen las reglas de cómo se van a notificar cambios en el expediente a las partes involucradas. Se habla de cómo los efectos de la notificación

tienen lugar en el mismo día en que se practique. También se señala la forma en que las mismas pueden efectuarse: en persona, por correo certificado, medios digitales o sistemas autorizados como lo es el Portal Nacional de Transparencia, correo postal ordinario o correo electrónico ordinario y "estrados" que se tienen como el lugar visible que tienen las instituciones (en este caso el INAI o los garantes locales) que se tiene para efecto de poner comunicaciones al público. El cómputo de los plazos en los recursos surte efectos al día siguiente de la notificación (artículo 99).

El INAI o los garantes locales pueden pedir información ("requerir") al titular, al responsable y a otros (artículo 100), cualquier negativa de atender o cumplimentar requerimientos, solicitudes u otros implica la pérdida del derecho de hacer valer información en otras partes del procedimiento y la autoridad hará su resolución con la información que tenga a la mano (artículo 101).

Las pruebas son aquellos medios a disposición de la autoridad para valorar la certeza de los hechos que se afirman en el recurso y pueden ofrecer las partes en el recurso. El artículo 102 establece cuáles son las pruebas procedentes en los recursos: documental pública (documentos de valor público, como los que expide el gobierno o certifican los notarios), documental privada (no tienen valor público), la inspección, la pericial (opiniones de expertos o "peritos"), la testimonial (un tercero declara), la confesional (se hace un pliego de preguntas a un testigo), elementos aportados por la ciencia y tecnología y las presunciones que existen de ley *(iura et de iure)* y salvo prueba en contrario *(iuris tantum),* que se denominan legal y humana.

El artículo 103 establece la posibilidad del solicitante de acudir al recurso de revisión directamente o por medio de representante ante el órgano garante contra el sujeto obligado, dentro del plazo de quince días posteriores a la notificación de la resolución o de la omisión en la emisión de la misma contra la que se está quejando.

El recurso se puede presentar por medios electrónicos o directamente ante la Unidad de Transparencia, y ésta debe remitir el recurso al garante un día después de haberlo recibido.

El recurso de revisión se puede usar en contra de la clasificación de datos personales que no cumplan las características de Ley, la inexistencia de datos personales, la incompetencia por el responsable, la entrega de datos personales incompletos, la entrega de datos personales que no correspondan con lo solicitado, la negativa de acceso; rectificación, cancelación u oposición de datos personales, que no se dé respuesta a una solicitud para el ejercicio de los derechos ARCO, que se entreguen datos en una modalidad o formato distinta a lo solicitado, la inconformidad con los costos de reproducción, envío o tiempos de entrega de los datos personales; el que se obstaculice el ejercicio de los derechos ARCO, que no se dé trámite a una solicitud para el ejercicio de los derechos ARCO, entre otros casos que dispone la legislación (artículo 104).

En el artículo 105, se listan los requisitos del escrito de interposición: se debe señalar el área responsable, el nombre del titular, la fecha en que fue notificada la respuesta al titular, el acto que se recurre y los puntos petitorios, la copia de la respuesta que se impugna y la notificación correspondiente y se debe acreditar propiamente la identidad del titular y la personalidad e identidad del representante, si lo hubiera. El recurso de revisión no se necesita ratificar.

La Ley contempla que, al admitirse el recurso de revisión, puede haber una fase de conciliación entre el titular y el responsable y mediada por el INAI o el garante local en el caso que se esté tratando; si de este procedimiento resulta un acuerdo, éste se plasma en un escrito y tiene efectos vinculantes (artículo 106).

El procedimiento de conciliación es el siguiente: se hace un requerimiento de conciliación por parte de la autoridad y, si las partes lo deciden, puede haber una audiencia de conciliación, de forma presencial o por comunicación electrónica; el conciliador podrá pedir pruebas, dentro de cinco días, cuando lo estime necesario y puede también, bajo ese mismo criterio decretar la suspensión de la audiencia, reanudando a más tardar en cinco días. Toda audiencia de conciliación debe tener un acta respectiva y, si no existe un acuerdo, el procedimiento sigue (artículos 107 y 108).

Los recursos deben resolverse dentro de un lapso de cuarenta días y en el mismo opera la suplencia de la deficiencia de la queja, es decir, que la autoridad de iniciativa propia subsane los errores contemplados por parte del titular dentro del procedimiento. Esto surge del juicio de amparo y se importa a este procedimiento protector de derechos humanos (artículo 109). No obstante, a partir de lo anterior, hay omisiones en el escrito que sólo pueden subsanarse por el titular y, por lo tanto, se le debe requerir por escrito, teniendo él mismo cinco días después de la notificación para hacerlo, so pena de que se deseche el escrito (artículo 110).

La resolución del recurso puede tener los siguientes esfuerzos: sobreseer (resolver como improcedente sin entrar al fondo) o desechar el escrito, confirmar la respuesta del responsable, revocar o modificar y ordenar la entrega de los datos personales. Las resoluciones deben establecer los plazos para su cumplimiento y si no hay una resolución, se tiene implícitamente confirmada la respuesta del responsable (artículo 111).

El artículo 112 establece las causales de improcedencia, si se presentan en un escrito de recurso de revisión, éste puede desecharse al recibirlo el órgano garante. Las causales son las siguientes: presentar el escrito fuera de los plazos que señala la Ley (“extemporaneidad”), no acreditar debidamente la identidad del titular, que exista una resolución definitiva sobre el mismo tema o no exista tema para plantear el recurso; que se esté tramitando un recurso en otra instancia, modificar o ampliar la petición y no exista interés jurídico. Sin embargo, desechar un recurso no implica que el titular pierde su derecho de volverlo a presentar.

En el 113, se habla de las causales de sobreseimiento, éstas significan que una vez admitido el recurso, hay una causa posterior que lo invalida y amerita su desecho (a esto se le llama sobreseimiento). Las causales son el desistimiento expreso del recurrente, su muerte, que haya aparecido después de admitido una causal de improcedencia (causal de improcedencia superviniente), la revocación o modificación de la respuesta de la responsable, que no exista tema para plantear el recurso (en la práctica se le dice "falta de materia").

Las resoluciones de los recursos deben notificarse y publicarse a más tardar al tercer día de su aprobación, estas resoluciones deberán ser vinculantes, definitivas e inatacables para los responsables. Los titulares pueden inconformarse de dichas resoluciones por medio del juicio de amparo (artículos 114 y 115). En el caso de las resoluciones de recursos de revisión realizadas a nivel local, se puede acudir al INAI por medio del recurso de inconformidad, aunque como se dijo, procede también el juicio de amparo (artículo 116).

El artículo 117 establece aspectos particulares del recurso de inconformidad como el plazo para presentarse (quince días después de la resolución impugnada) y el trámite que debe seguir, donde el garante local debe enviar al INAI el recurso de inconformidad al día siguiente de haberlo recibido. En el numeral 118, se muestra las causas por las que se considera procedente este recurso: la mala clasificación de los datos, la inexistencia de los mismos, la entrega de datos personales incompletos, la de datos personales que no correspondan con lo solicitado, la negativa de acceso, rectificación, cancelación u oposición, la entrega de los datos en un formato incomprensible, la inconformidad con los costos de reproducción, envío, o tiempos de entrega y la contravención de las disposiciones del artículo 54.

El artículo 119 establece que el escrito de interposición debe cumplir con lo siguiente: área responsable ante la cual se presentó la solicitud para el ejercicio de los derechos ARCO, el organismo garante que emitió la resolución impugnada, el recurrente o su representante, la fecha de notificación de la resolución, el acto que se recurre, puntos petitorios y razones de inconformidad, la copia de la resolución, la acreditación de la identidad del titular y cualquier prueba o elemento de convicción que se considere procedente. El artículo 120 señala que la resolución del recurso de inconformidad no puede exceder de treinta días después de la presentación (interposición en términos jurídicos).

De la misma forma que en el recurso de revisión, en la inconformidad opera también la suplencia de la queja, siempre y cuando "no altere el contenido original del recurso de inconformidad, ni modifique los hechos o peticiones expuestas en el mismo" y, de la misma forma, se puede hacer el requerimiento al titular por omisiones en el escrito, con el mismo plazo de prevención y los mismos efectos (artículos 121

y 122). Una vez que se acaba el ofrecimiento de pruebas, el expediente se pone a disposición de las partes para que en cinco días hagan alegatos (artículo 123); en la práctica, puede ser uno oral o escrito.

Como en el recurso de revisión, los efectos de la resolución del recurso de inconformidad son el sobreseimiento o desecho, confirmación de la resolución del organismo garante, revocación o modificación y entrega de los datos personales, estableciendo los plazos de cumplimiento de la resolución y, si no hubiera resolución, se entiende por confirmada la del garante local (artículo 124).

Son causas de improcedencia (causales en términos jurídicos) del recurso de inconformidad, los siguientes: extemporaneidad, la existencia de resolución definitiva sobre el mismo tema, que el recurso no tenga materia, que se encuentre tramitado un recurso en otra instancia (como lo sería el Poder Judicial) y se amplíe la solicitud (artículo 125). Como causales de sobreseimiento tenemos el desistimiento expreso, el fallecimiento del recurrente, la revocación o modificación de la respuesta del responsable o una causal de improcedencia posterior.

Si el recurso de inconformidad modifica o revoca la resolución del órgano garante, éste debe emitir un nuevo fallo con los lineamientos fijados (artículo 127). El garante local deberá también dar seguimiento y vigilancia del cumplimiento de la nueva resolución que hagan (artículo 128). Como en el recurso de revisión, las resoluciones son vinculantes, definitivas e inatacables para los responsables y los Organismos garantes y procede su impugnación por medio del juicio de amparo (artículo 129).

El Instituto Nacional de Transparencia y Acceso a la Información Pública tiene la facultad de atraer recursos de revisión que estén tramitando los garantes locales, el criterio para poderlo hacer es el "interés y la trascendencia"; además, se establece que este instituto puede establecer lineamientos sobre recursos de revisión de interés o relevancia. En éstos, debe atender a los siguientes factores: finalidad del tratamiento de los datos personales, el número o tipo de titulares, la sensibilidad de los datos tratados, las posibles consecuencias y la relevancia del tratamiento de datos personales en atención a su impacto (artículo 130).

Cuando decida ejercer la atracción, el Instituto debe de realizar un estudio previo donde hagan la fundamentación y motivación debidas. Se establecen claramente los criterios que lo deben informar: "…el caso es de tal relevancia, novedad o complejidad, que su resolución podrá repercutir de manera sustancial en la solución de casos futuros para garantizar la tutela efectiva del derecho de acceso a la información." Ésta se debe notificar al garante local en un plazo no mayor a tres días (artículo 131 y 132).

Es importante notar cómo la justificación de la atracción es un estudio previo y no es parte del análisis de fondo que se realiza al resolver el recurso (Artículo 132). Además, el Instituto debe contar con lineamientos y criterios para determinar el

interés y la trascendencia (Artículo 134). El artículo 134 también establece las reglas para ejercer la facultad de atracción: existe la atracción de oficio, pero los garantes locales pueden hacer una petición de atracción en cinco días, si pasan el tiempo y no se hace, se tiene por precluída esta facultad del garante local. El Instituto tiene diez días para determinar si atrae o no el recurso.

La solicitud de atracción interrumpe el plazo de resolución del recurso de revisión y éste prosigue si el Instituto decide no atraerla (Artículo 135). Antes de que el Instituto se pronuncie sobre la procedencia de la atracción, el garante local que conozca del recurso debe hacer un análisis de fondo de los temas que no sean de importancia y trascendencia para la atracción (Artículo 136). Si se atrae, el Instituto debe estudiar el fondo del recurso atraído. La resolución que se haga sobre el recurso atraído es definitiva e inatacable para el organismo garante local y el sujeto obligado. Procede la vía de amparo para el ciudadano que se encuentre inconforme (Artículo 137).

Los artículos 138 y 139 versan sobre el recurso de revisión en materia de seguridad nacional, cuya interposición es facultad exclusiva del Consejero Jurídico del Gobierno y se lleva a cabo ante la Suprema Corte de Justicia de la Nación, en el caso de que las resoluciones del Instituto de sus recursos pongan en peligro la seguridad nacional. Éste debe interponerse dentro de siete días después de la notificación que se haga al sujeto obligado del recurso y, al recibirlo, la Corte suspenderá la ejecución de inmediato para ahí proceder a admitir o rechazar el recurso dentro del plazo de cinco días.

El recurso debe señalar la forma en cómo se pone en peligro la seguridad nacional, debiendo fundamentar y motivar y aportando las pruebas necesarias para ello (Artículo 140). En el artículo 141, se habla del tratamiento de la información confidencial que la Suprema Corte puede pedir para resolver el asunto y el acceso de los ministros a la información clasificada. El 142 establece la jurisdicción plena de la Suprema Corte y el 143 prevé lo que hace éste órgano en caso de confirmar o revocar la resolución.

El artículo 144 establece los criterios de interpretación que puede emitir el INAI cuando la resolución de sus recursos haya terminado de surtir sus efectos (en términos jurídicos, causado ejecutoria o causado estado). Éstos son de carácter orientador y se establecen al resolver de la misma manera y de forma consecutiva tres casos similares, con una votación de dos terceras partes de todos los consejeros del Instituto (es decir, de su Pleno) El criterio de interpretación debe tener un rubro, es decir, el título de la resolución que resume el contenido de la misma, un texto donde viene el punto medular del criterio y los precedentes que hayan dado lugar al criterio. Asimismo, deben tener una clave de control para su registro adecuado.

CAPÍTULO I
DISPOSICIONES COMUNES A LOS RECURSOS DE REVISIÓN Y RECURSOS DE INCONFORMIDAD

RECURSO DE REVISIÓN O DE INCONFORMIDAD

Artículo 94. El titular o su representante podrá interponer un recurso de revisión o un recurso de inconformidad ante el Instituto o los Organismos garantes, según corresponda, o bien, ante la Unidad de Transparencia, a través de los siguientes medios **(medios de interposición)**:

I. Escrito libre: Por escrito libre en el domicilio del Instituto o los Organismos garantes, según corresponda, o en las oficinas habilitadas que al efecto establezcan;

II. Correo certificado: Por correo certificado con acuse de recibo;

III. Formatos que emita el Instituto y organismos garantes: Por formatos que al efecto emita el Instituto o los Organismos garantes, según corresponda;

IV. Medios electrónicos: Por los medios electrónicos que para tal fin se autoricen, o

V. Otros medios: Cualquier otro medio que al efecto establezca el Instituto o los Organismos garantes, según corresponda.

Se presumirá que el titular acepta que las notificaciones le sean efectuadas por el mismo conducto que presentó su escrito, salvo que acredite haber señalado uno distinto para recibir notificaciones.

IDENTIDAD DEL TITULAR. MEDIOS DE ACREDITACIÓN

Artículo 95. El titular podrá acreditar su identidad a través de cualquiera de los siguientes medios:

I. Identificación oficial: Identificación oficial;

II. Firma electrónica: Firma electrónica avanzada o del instrumento electrónico que lo sustituya, o

III. Mecanismos de autenticación autorizados: Mecanismos de autenticación autorizados por el Instituto y los Organismos garantes, según corresponda, publicados mediante acuerdo general en el Diario Oficial de la Federación o en los diarios y gacetas oficiales de las Entidades Federativas.

USO DE LA FIRMA ELECTRÓNICA

La utilización de la firma electrónica avanzada o del instrumento electrónico que lo sustituya eximirá de la presentación de la copia del documento de identificación.

ACREDITACIÓN DEL REPRESENTANTE

Artículo 96. Cuando el titular actúe mediante un representante, éste deberá acreditar su personalidad en los siguientes términos:

I. Persona física: Si se trata de una persona física, a través de carta poder simple suscrita ante dos testigos anexando copia de las identificaciones de los suscriptores, o instrumento público, o declaración en comparecencia personal del titular y del representante ante el Instituto.

II. Persona moral: Si se trata de una persona moral, mediante instrumento público.

RECURSOS RESPECTO DE DATOS DE PERSONAS FALLECIDAS

Artículo 97. La interposición de un recurso de revisión o de inconformidad de datos personales concernientes a personas fallecidas, podrá realizarla la persona que acredite tener un interés jurídico o legítimo.

NOTIFICACIONES

Artículo 98. En la sustanciación de los recursos de revisión y recursos de inconformidad, las notificaciones que emitan el Instituto y los Organismos garantes, según corresponda, surtirán efectos el mismo día en que se practiquen.

FORMA DE EFECTUARSE

Las notificaciones podrán efectuarse:

I. Personal: Personalmente en los siguientes casos:

a) Primera notificación: Se trate de la primera notificación;

b) Requerimiento de un acto a la parte que deba cumplirlo: Se trate del requerimiento de un acto a la parte que deba cumplirlo;

c) Solicitud de informes o documentos: Se trate de la solicitud de informes o documentos;

d) Resolución que ponga fin a procedimiento: Se trate de la resolución que ponga fin al procedimiento de que se trate, y

e) Cláusula residual: En los demás casos que disponga la ley;

II. Por correo certificado, medios digitales o sistemas autorizados: Por correo certificado con acuse de recibo o medios digitales o sistemas autorizados por el Instituto o los Organismos garantes, según corresponda, y publicados mediante acuerdo general en el Diario Oficial de la Federación o diarios o gacetas oficiales de las Entidades Federativas, cuando se trate de requerimientos, emplazamientos, solicitudes de informes o documentos y resoluciones que puedan ser impugnadas;

III. Correo postal ordinario o correo electrónico ordinario: Por correo postal ordinario o por correo electrónico ordinario cuando se trate de actos distintos de los señalados en las fracciones anteriores, o

IV. Estrados: Por estrados, cuando la persona a quien deba notificarse no sea localizable en su domicilio, se ignore éste o el de su representante.

CÓMPUTO DE PLAZOS

Artículo 99. El cómputo de los plazos señalados en el presente Título comenzará a correr a partir del día siguiente a aquél en que haya surtido efectos la notificación correspondiente.

Concluidos los plazos fijados a las partes, se tendrá por perdido el derecho que dentro de ellos debió ejercitarse, sin necesidad de acuse de rebeldía por parte del Instituto.

REQUERIMIENTOS DE INFORMACIÓN

Artículo 100. El titular, el responsable y los Organismos garantes o cualquier autoridad deberán atender los requerimientos de información en los plazos y términos que el Instituto y los Organismos garantes, según corresponda, establezcan.

NEGATIVA DE ATENDER O CUMPLIMENTAR REQUERIMIENTOS, SOLICITUDES U OTROS

Artículo 101. Cuando el titular, el responsable, los Organismos garantes o cualquier autoridad se nieguen a atender o cumplimentar los requerimientos, solicitudes de información y documentación, emplazamientos, citaciones o diligencias notificadas por

el Instituto o los Organismos garantes, según corresponda, o facilitar la práctica de las diligencias que hayan sido ordenadas, o entorpezca las actuaciones del Instituto o los Organismos garantes, según corresponda, tendrán por perdido su derecho para hacerlo valer en algún otro momento del procedimiento y el Instituto y los Organismos garantes, según corresponda, tendrán por ciertos los hechos materia del procedimiento y resolverá con los elementos que disponga.

PRUEBAS PROCEDENTES EN LOS RECURSOS

Artículo 102. En la sustanciación de los recursos de revisión o recursos de inconformidad, las partes podrán ofrecer las siguientes pruebas:

I. Documental pública: La documental pública;

II. Documental privada: La documental privada;

III. Inspección: La inspección;

IV. Pericial: La pericial;

V. Testimonial: La testimonial;

VI. Confesional: La confesional, excepto tratándose de autoridades;

VII. Elementos aportados por la ciencia y tecnología: Las imágenes fotográficas, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología, y

VIII. Presuncional: La presuncional legal y humana.

OTROS MEDIOS DE PRUEBA

El Instituto y los Organismos garantes, según corresponda, podrán allegarse de los medios de prueba que consideren necesarios, sin más limitación que las establecidas en la ley.

CAPÍTULO II
DEL RECURSO DE REVISIÓN ANTE EL INSTITUTO Y LOS ORGANISMOS GARANTES

RECURSO DE REVISIÓN

Artículo 103. El titular, por sí mismo o a través de su representante, podrán interponer un recurso de revisión ante el Instituto o, en su caso, ante los Organismos garantes o la Unidad de Transparencia del responsable que haya conocido de la solicitud **(órgano competente)** para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta **(plazo)**.

POR OMISIÓN ADMINISTRATIVA

Transcurrido el plazo previsto para dar respuesta a una solicitud para el ejercicio de los derechos ARCO sin que se haya emitido ésta, el titular o, en su caso, su representante podrán interponer el recurso de revisión dentro de los quince días siguientes al que haya vencido el plazo para dar respuesta.

CASOS DE PROCEDENCIA

Artículo 104. El recurso de revisión procederá en los siguientes supuestos:

I. Se clasifiquen como confidenciales datos personales que no cumplan las características de Ley: Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

II. Inexistencia de datos personales: Se declare la inexistencia de los datos personales;

III. Incompetencia por el responsable: Se declare la incompetencia por el responsable;

IV. Datos personales incompletos: Se entreguen datos personales incompletos;

V. Datos personales que no correspondan con lo solicitado: Se entreguen datos personales que no correspondan con lo solicitado;

VI. Negativa de acceso, rectificación, cancelación u oposición de datos personales: 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: 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 entreguen datos en una modalidad o formato distinta a lo solicitado: Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;

IX. Inconformidad con los costos de reproducción, envío o tiempos de entrega de los datos personales: 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: 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: No se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y

XII. Cláusula residual: En los demás casos que dispongan las leyes.

REQUISITOS DEL ESCRITO DE INTERPOSICIÓN

Artículo 105. Los únicos requisitos exigibles en el escrito de interposición del recurso de revisión serán los siguientes:

I. Área responsable: El área responsable ante quien se presentó la solicitud para el ejercicio de los derechos ARCO;

II. Nombre del titular: El nombre del titular que recurre o su representante y, en su caso, del tercero interesado, así como el domicilio o medio que señale para recibir notificaciones;

III. Fecha en que fue notificada la respuesta al titular: La fecha en que fue notificada la respuesta al titular, o bien, en caso de falta de respuesta la fecha de la presentación de la solicitud para el ejercicio de los derechos ARCO;

IV. Acto que se recurre y los puntos petitorios: El acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad;

V. Copia de la respuesta que se impugna y la notificación correspondiente: En

su caso, copia de la respuesta que se impugna y de la notificación correspondiente, y

VI. Identidad del titular y la personalidad e identidad del representante: Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.

PRUEBAS

Al recurso de revisión se podrán acompañar las pruebas y demás elementos que considere el titular procedentes someter a juicio del Instituto o, en su caso, de los Organismos garantes.

EL RECURSO DE REVISIÓN NO SE NECESITA RATIFICAR

En ningún caso será necesario que el titular ratifique el recurso de revisión interpuesto.

FASE DE CONCILIACIÓN

Artículo 106. Una vez admitido el recurso de revisión, el Instituto o, en su caso, los Organismos garantes podrán buscar una conciliación entre el titular y el responsable.

ACUERDO DE CONCILIACIÓN

De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes (forma y efectos). El recurso de revisión quedará sin materia y el Instituto, o en su caso, los Organismos garantes, deberán verificar el cumplimiento del acuerdo respectivo (cumplimiento).

PROCEDIMIENTO DE CONCILIACIÓN

Artículo 107. Admitido el recurso de revisión y sin perjuicio de lo dispuesto por el artículo 65 de la presente Ley, el Instituto promoverá la conciliación entre las partes, de conformidad con el siguiente procedimiento:

I. Requerimiento de conciliación: El Instituto y los Organismos garantes, según corresponda, requerirán a las partes que manifiesten, por cualquier medio, su voluntad de conciliar, en un plazo no mayor a siete días **(plazo)**, contados a partir de la notificación de dicho acuerdo, mismo que contendrá un resumen del recurso de revisión y de la respuesta del responsable si la hubiere, señalando los elementos comunes y los puntos de controversia.

a) Formas en cómo se realice: La conciliación podrá celebrarse

presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el Instituto o los Organismos garantes, según corresponda. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.

b) Excepción: Queda exceptuado de la etapa de conciliación, cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con la Ley y el Reglamento, salvo que cuente con representación legal debidamente acreditada;

II. Audiencia de conciliación: Aceptada la posibilidad de conciliar por ambas partes, el Instituto y los Organismos garantes, según correspondan, señalarán el lugar o medio, día y hora para la celebración de una audiencia de conciliación, la cual deberá realizarse dentro de los diez días siguientes en que el Instituto o los Organismos garantes, según corresponda, hayan recibido la manifestación de la voluntad de conciliar de ambas partes, en la que se procurará avenir los intereses entre el titular y el responsable.

a) Elementos de convicción: El conciliador podrá, en todo momento en la etapa de conciliación, requerir a las partes que presenten en un plazo máximo de cinco días, los elementos de convicción que estime necesarios para la conciliación **(plazos para aportarlos)**.

b) Suspensión de la audiencia: El conciliador podrá suspender cuando lo estime pertinente o a instancia de ambas partes la audiencia por una ocasión. En caso de que se suspenda la audiencia, el conciliador señalará día y hora para su reanudación dentro de los cinco días siguientes.

c) Levantamiento de actas: De toda audiencia de conciliación se levantará el acta respectiva, en la que conste el resultado de la misma. En caso de que el responsable o el titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa;

III. Falta justificada: Si alguna de las partes no acude a la audiencia de conciliación y justifica su ausencia en un plazo de tres días, será convocado a una segunda audiencia de conciliación, en el plazo de cinco días; en caso de que no acuda a esta última, se continuará con el recurso de revisión. Cuando alguna de las partes no acuda a la audiencia de conciliación sin justificación alguna, se continuará con el procedimiento **(falta injustificada)**;

IV. Falta de acuerdo: De no existir acuerdo en la audiencia de conciliación, se continuará con el recurso de revisión;

V. Acuerdo: De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto, o en su caso, los Organismos garantes, deberán verificar el cumplimiento del acuerdo respectivo, y

VI. Cumplimiento del acuerdo: El cumplimiento del acuerdo dará por concluido la sustanciación del recurso de revisión, en caso contrario, el Instituto reanudará el procedimiento.

TEMPORALIDAD DE LA CONCILIACIÓN

El plazo al que se refiere el artículo siguiente de la presente Ley será suspendido durante el periodo de cumplimiento del acuerdo de conciliación.

PLAZO DE LA RESOLUCIÓN DEL RECURSO

Artículo 108. El Instituto y los Organismos garantes resolverán el recurso de revisión en un plazo que no podrá exceder de cuarenta días, el cual podrá ampliarse hasta por veinte días por una sola vez.

SUPLENCIA DE LA DEFICIENCIA DE LA QUEJA

Artículo 109. Durante el procedimiento a que se refiere el presente Capítulo, el Instituto y los Organismos garantes, según corresponda, deberán aplicar la suplencia de la queja a favor del titular, siempre y cuando no altere el contenido original del recurso de revisión, ni modifique los hechos o peticiones expuestas en el mismo, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones **(parámetros)**.

REQUERIMIENTO AL TITULAR POR OMISIONES EN EL ESCRITO

Artículo 110. Si en el escrito de interposición del recurso de revisión el titular no cumple con alguno de los requisitos previstos en el artículo 105 de la presente Ley y el Instituto y los Organismos garantes, según corresponda, no cuenten con elementos para subsanarlos, éstos deberán requerir al titular, por una sola ocasión, la información que subsane las omisiones en un plazo que no podrá exceder de cinco días, contados a partir del día siguiente de la presentación del escrito.

PLAZO DE LA PREVENCIÓN

El titular contará con un plazo que no podrá exceder de cinco días, contados a partir del día siguiente al de la notificación de la prevención, para subsanar las omisiones, con el apercibimiento de que en caso de no cumplir con el requerimiento, se desechará el recurso de revisión.

EFECTOS DE LA PREVENCIÓN (TEMPORALIDAD)

La prevención tendrá el efecto de interrumpir el plazo que tienen el Instituto y los Organismos garantes para resolver el recurso, por lo que comenzará a computarse a partir del día siguiente a su desahogo.

EFECTOS DE LA RESOLUCIÓN DEL RECURSO

Artículo 111. Las resoluciones del Instituto o, en su caso, de los Organismos garantes podrán:

I. Sobreseer o desechar: Sobreseer o desechar el recurso de revisión por improcedente;

II. Confirmar: Confirmar la respuesta del responsable;

III. Revocar o modificar: Revocar o modificar la respuesta del responsable, o

IV. Ordenar la entrega de los datos personales: Ordenar la entrega de los datos personales, en caso de omisión del responsable.

PLAZOS DE CUMPLIMIENTO DE LA RESOLUCIÓN

Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los responsables deberán informar al Instituto o, en su caso, a los Organismos garantes el cumplimiento de sus resoluciones.

FALTA DE RESOLUCIÓN. EFECTOS

Ante la falta de resolución por parte del Instituto, o en su caso, de los Organismos garantes, se entenderá confirmada la respuesta del responsable.

PROBABLE RESPONSABILIDAD

Cuando el Instituto, o en su caso, los Organismos garantes, determinen durante la sustanciación del recurso de revisión que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente Ley

y demás disposiciones que resulten aplicables en la materia, deberán hacerlo del conocimiento del órgano interno de control o de la instancia competente para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo.

CAUSALES DE IMPROCEDENCIA

Artículo 112. El recurso de revisión podrá ser desechado por improcedente cuando:

I. Extemporaneidad: Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 103 de la presente Ley;

II. Falta de identidad: El titular o su representante no acrediten debidamente su identidad y personalidad de este último;

III. Resolución definitiva sobre el mismo tema: El Instituto o, en su caso, los Organismos garantes hayan resuelto anteriormente en definitiva sobre la materia del mismo;

IV. No exista materia del recurso: No se actualice alguna de las causales del recurso de revisión previstas en el artículo 104 de la presente Ley;

V. Trámite de un recurso en otra instancia: Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el recurrente, o en su caso, por el tercero interesado, en contra del acto recurrido ante el Instituto o los Organismos garantes, según corresponda;

VI. Modificación o ampliación de la petición: El recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos, o

VII. Falta de interés jurídico: El recurrente no acredite interés jurídico.

EL DESECHAMIENTO NO IMPLICA LA PRECLUSIÓN DEL DERECHO DEL TITULAR

El desechamiento no implica la preclusión del derecho del titular para interponer ante el Instituto o los Organismos garantes, según corresponda, un nuevo recurso de revisión.

CAUSALES DE SOBRESEIMIENTO

Artículo 113. El recurso de revisión solo podrá ser sobreseído cuando:

I. Desistimiento: El recurrente se desista expresamente;

II. Fallecimiento: El recurrente fallezca;

III. Causal de improcedencia superviniente: Admitido el recurso de revisión, se actualice alguna causal de improcedencia en los términos de la presente Ley;

IV. Revocación o modificación de la respuesta de la responsable: El responsable modifique o revoque su respuesta de tal manera que el recurso de revisión quede sin materia, o

V. Falta de materia: Quede sin materia el recurso de revisión.

NOTIFICACIÓN DE LAS RESOLUCIONES

Artículo 114. El Instituto y los Organismos garantes deberán notificar a las partes y publicar las resoluciones, en versión pública, a más tardar, al tercer día siguiente de su aprobación.

CARACTERÍSTICA DE LAS RESOLUCIONES

Artículo 115. Las resoluciones del Instituto y de los Organismos garantes serán vinculantes, definitivas e inatacables para los responsables.

PROCEDENCIA DE LA VÍA DE AMPARO

Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el Juicio de Amparo.

PROCEDENCIA DEL RECURSO DE INCONFORMIDAD

Artículo 116. Tratándose de las resoluciones a los recursos de revisión de los Organismos garantes de las Entidades Federativas, los particulares podrán optar por acudir ante el Instituto interponiendo el recurso de inconformidad previsto en esta Ley o ante el Poder Judicial de la Federación mediante el Juicio de Amparo.

CAPÍTULO III
DEL RECURSO DE INCONFORMIDAD ANTE EL INSTITUTO

RECURSO DE INCONFORMIDAD

Artículo 117. El titular, por sí mismo o a través de su representante, podrá impugnar la resolución del recurso de revisión emitido por el organismo garante ante el Instituto, mediante el recurso de inconformidad.

PRESENTACIÓN Y PLAZO

El recurso de inconformidad se podrá presentar ante el organismo garante que haya emitido la resolución o ante el Instituto, dentro de un plazo de quince días contados a partir del siguiente a la fecha de la notificación de la resolución impugnada.

TRÁMITE

Los Organismos garantes deberán remitir el recurso de inconformidad al Instituto al día siguiente de haberlo recibido; así como las constancias que integren el procedimiento que haya dado origen a la resolución impugnada, el cual resolverá allegándose de los elementos que estime convenientes.

CAUSALES DE PROCEDENCIA

Artículo 118. El recurso de inconformidad procederá contra las resoluciones emitidas por los Organismos garantes de las Entidades Federativas que:

I. Mala clasificación de los datos: Clasifiquen los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

II. Inexistencia de los datos: Determinen la inexistencia de datos personales, o

III. Negativa de los datos personales: Declaren la negativa de datos personales,

es decir:

a) Datos personales incompletos: Se entreguen datos personales incompletos;

b) Datos personales que no correspondan con lo solicitado: Se entreguen datos personales que no correspondan con los solicitados;

c) Negativa de acceso, rectificación, cancelación u oposición: Se niegue el acceso, rectificación, cancelación u oposición de datos personales;

d) Se entregue en un formato incomprensible: Se entregue o ponga a disposición datos personales en un formato incomprensible;

e) El titular se inconforme con los costos de reproducción, envío, o tiempos de entrega: El titular se inconforme con los costos de reproducción, envío, o tiempos de entrega de los datos personales, o

f) Se contravenga lo dispuesto por el artículo 54: Se oriente a un trámite específico que contravenga lo dispuesto por el artículo 54 de la presente Ley.

REQUISITOS DEL ESCRITO DE INTERPOSICIÓN

Artículo 119. Los únicos requisitos exigibles e indispensables en el escrito de interposición del recurso de inconformidad son:

I. Responsable: El área responsable ante la cual se presentó la solicitud para el ejercicio de los derechos ARCO;

II. Organismos garante: El organismo garante que emitió la resolución impugnada;

III. Recurrente o representante: El nombre del titular que recurre o de su representante y, en su caso, del tercero interesado, así como su domicilio o el medio que señale para recibir notificaciones;

IV. Fecha de notificación de la resolución: La fecha en que fue notificada la resolución al titular;

V. Acto que se recurre, puntos petitorios y razones de inconformidad: El acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad;

VI. Copia de la resolución: En su caso, copia de la resolución que se impugna y de la notificación correspondiente, y

VII. Identidad del titular: Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.

PRUEBAS Y ELEMENTOS DE CONVICCIÓN

El promovente podrá acompañar su escrito con las pruebas y demás elementos que considere procedentes someter a juicio del Instituto.

PLAZO DE RESOLUCIÓN

Artículo 120. El Instituto resolverá el recurso de inconformidad en un plazo que no podrá exceder de treinta días contados a partir del día siguiente de la interposición del recurso de inconformidad, plazo que podrá ampliarse por una sola vez y hasta por un periodo igual **(ampliación)**.

SUPLENCIA DE LA QUEJA

Artículo 121. Durante el procedimiento a que se refiere el presente Capítulo, el Instituto deberá aplicar la suplencia de la queja a favor del titular, siempre y cuando no altere el contenido original del recurso de inconformidad, ni modifique los hechos o peticiones expuestas en el mismo, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones **(parámetros)**.

REQUERIMIENTO AL TITULAR POR OMISIONES EN EL ESCRITO

Artículo 122. Si en el escrito de interposición del recurso de inconformidad el titular no cumple con alguno de los requisitos previstos en el artículo 119 de la presente Ley y el Instituto no cuente con elementos para subsanarlos, éste deberá requerir al titular, por una sola ocasión, la información que subsane las omisiones en un plazo que no podrá exceder de cinco días, contados a partir del día siguiente de la presentación del escrito.

PLAZO DE PREVENCIÓN

El titular contará con un plazo que no podrá exceder de quince días, contados a partir del día siguiente al de la notificación de la prevención, para subsanar las omisiones, con el apercibimiento de que en caso de no cumplir con el requerimiento, se desechará el recurso de inconformidad.

EFECTOS DE LA PREVENCIÓN (TEMPORALIDAD)

La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver el recurso, por lo que comenzará a computarse a partir del día siguiente a su desahogo.

ALEGATOS

Artículo 123. Una vez concluida la etapa probatoria, el Instituto pondrá a disposición de las partes las actuaciones del procedimiento y les otorgará un plazo de cinco días para que formulen alegatos contados a partir de la notificación del acuerdo a que se refiere este artículo.

EFECTOS DE LA RESOLUCIÓN DEL RECURSO

Artículo 124. Las resoluciones del Instituto podrán:

I. Sobreseimiento o desechamiento: Sobreseer o desechar el recurso de inconformidad;

II. Confirmación: Confirmar la resolución del organismo garante;

III. Revocación o modificación: Revocar o modificar la resolución del organismo garante, o

IV. Entrega de los datos personales: Ordenar la entrega de los datos personales, en caso de omisión del responsable.

PLAZOS DE CUMPLIMIENTO DE LA RESOLUCIÓN

Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los Organismos garantes deberán informar al Instituto sobre el cumplimiento de sus resoluciones.

FALTA DE RESOLUCIÓN. EFECTOS.

Si el Instituto no resuelve dentro del plazo establecido en este Capítulo, la resolución que se recurrió se entenderá confirmada.

PROBABLE RESPONSABILIDAD

Cuando el Instituto determine durante la sustanciación del recurso de inconformidad, que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente Ley y a las demás disposiciones aplicables en la materia, deberá hacerlo del conocimiento del órgano interno de control o de la instancia competente para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo.

APREMIO PARA EL CUMPLIMIENTO DE LAS RESOLUCIONES

Las medidas de apremio previstas en la presente Ley, resultarán aplicables para efectos del cumplimiento de las resoluciones que recaigan a los recursos de inconformidad. Estas medidas de apremio deberán establecerse en la propia resolución.

CAUSALES DE IMPROCEDENCIA

Artículo 125. El recurso de inconformidad podrá ser desechado por improcedente cuando:

I. Extemporaneidad: Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 117 de la presente Ley;

II. Resolución definitiva sobre el mismo tema: El Instituto anteriormente haya resuelto en definitiva sobre la materia del mismo;

III. No exista materia del recurso: No se actualicen las causales de procedencia del recurso de inconformidad, previstas en el artículo 118 de la presente Ley;

IV. Trámite de un recurso en otra instancia: Se esté tramitando ante el Poder Judicial algún recurso o medio de defensa interpuesto por el titular, o en su caso, por el tercero interesado, en contra del acto recurrido, o

V. Ampliación de la solicitud: El inconforme amplíe su solicitud en el recurso de inconformidad, únicamente respecto de los nuevos contenidos.

CAUSALES DE SOBRESEIMIENTO

Artículo 126. El recurso de inconformidad solo podrá ser sobreseído cuando:

I. Desistimiento expreso: El recurrente se desista expresamente;

II. Fallecimiento: El recurrente fallezca;

III. Revocación o modificación de la respuesta del responsable: El organismo garante modifique o revoque su respuesta de tal manera que el recurso de inconformidad quede sin materia, o

IV. Causal de improcedencia superviniente: Admitido el recurso, se actualice alguna causal de improcedencia en los términos de la presente Ley.

NUEVO FALLO POR MODIFICACIÓN DE LA RESOLUCIÓN DEL GARANTE

Artículo 127. En los casos en que a través del recurso de inconformidad se modifique o revoque la resolución del organismo garante, éste deberá emitir un nuevo fallo atendiendo los lineamientos que se fijaron al resolver la inconformidad, dentro del plazo de quince días, contados a partir del día siguiente al en que se hubiere notificado o se tenga conocimiento de la resolución dictada en la inconformidad.

SEGUIMIENTO Y VIGILANCIA DEL CUMPLIMIENTO DE LA NUEVA RESOLUCIÓN

Artículo 128. Corresponderá a los Organismos garantes, en el ámbito de su competencia, realizar el seguimiento y vigilancia del debido cumplimiento por parte del responsable de la nueva resolución emitida como consecuencia de la inconformidad en términos de la presente Ley.

CARACTERÍSTICAS DE LAS RESOLUCIONES

Artículo 129. Las resoluciones del Instituto serán vinculantes, definitivas e inatacables para los responsables y los Organismos garantes.

PROCEDENCIA DE LA VÍA DE AMPARO

Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el Juicio de Amparo.

CAPÍTULO IV
DE LA ATRACCIÓN DE LOS RECURSOS DE REVISIÓN

FACULTAD DE ATRACCIÓN

Artículo 130. Para efectos de la presente Ley, el Pleno del Instituto, cuando así lo apruebe la mayoría de sus Comisionados, de oficio o a petición fundada de los Organismos garantes, podrá ejercer la facultad de atracción **(procedimiento)** para conocer de aquellos recursos de revisión pendientes de resolución en materia de protección de datos personales, que por su interés y trascendencia así lo ameriten y cuya competencia original corresponde a los Organismos garantes, conforme a lo dispuesto en esta Ley y demás normativa aplicable **(materia)**.

PETICIÓN DE ATRACCIÓN

Los recurrentes podrán hacer del conocimiento del Instituto la existencia de recursos de revisión que de oficio podría conocer.

LINEAMIENTOS SOBRE RECURSOS DE REVISIÓN DE INTERÉS O RELEVANCIA

Por lo que hace a los lineamientos y criterios generales de observancia obligatoria que el Instituto deberá emitir para determinar los recursos de revisión de interés y trascendencia que está obligado a conocer, conforme a la Ley General de Transparencia y Acceso a la Información Pública, adicionalmente en la atracción de recursos de revisión en materia de protección de datos personales se deberán considerar los siguientes factores **(factores)**:

I. Finalidad del tratamiento: La finalidad del tratamiento de los datos personales;

II. Número o tipo de titulares: El número y tipo de titulares involucrados en el tratamiento de datos personales llevado a cabo por el responsable;

III. Sensibilidad de los datos tratados: La sensibilidad de los datos personales tratados;

IV. Posibles consecuencias: Las posibles consecuencias que se derivarían de un tratamiento indebido o indiscriminado de datos personales, y

V. Relevancia del tratamiento de datos personales en atención a su impacto: La relevancia del tratamiento de datos personales, en atención al impacto social o económico del mismo y del interés público para conocer del recurso de revisión atraído.

FUNDAMENTACIÓN Y MOTIVACIÓN DEL EJERCICIO DE LA FACULTAD DE ATRACCIÓN

Artículo 131. Para efectos del ejercicio de la facultad de atracción a que se refiere este Capítulo, el Instituto motivará y fundamentará que el caso es de tal relevancia, novedad o complejidad, que su resolución podrá repercutir de manera sustancial en la solución de casos futuros para garantizar la tutela efectiva del derecho de protección de datos personales en posesión de sujetos obligados.

ATRACCIÓN CUANDO EL GARANTE SEA SUJETO OBLIGADO RECURRIDO

En los casos en los que el organismo garante de la Entidad Federativa sea el sujeto obligado recurrido, deberá notificar al Instituto, en un plazo que no excederá de tres días, a partir de que sea interpuesto el recurso. El Instituto atraerá y resolverá dichos recursos de revisión, conforme a lo establecido en el presente Capítulo.

NATURALEZA JURÍDICA DE LAS RAZONES PARA EJERCER LA FACULTAD DE ATRACCIÓN

Artículo 132. Las razones emitidas por el Instituto para ejercer la facultad de atracción de un caso, únicamente constituirán un estudio preliminar para determinar si el asunto reúne los requisitos constitucionales y legales de interés y trascendencia, conforme al precepto anterior, por lo que no será necesario que formen parte del análisis de fondo del asunto.

LINEAMIENTOS SOBRE RECURSOS DE REVISIÓN DE INTERÉS O RELEVANCIA

Artículo 133. El Instituto emitirá lineamientos y criterios generales de observancia obligatoria que permitan determinar los recursos de revisión de interés y trascendencia que estará obligado a conocer, así como los procedimientos internos para su tramitación, atendiendo a los plazos máximos señalados para el recurso de revisión.

REGLAS PARA EL EJERCICIO DE LA FACULTAD DE ATRACCIÓN

Artículo 134. La facultad de atracción conferida al Instituto se deberá ejercer conforme a las siguientes reglas:

I. Ejercicio oficioso: Cuando se efectúe de oficio, el Pleno del Instituto, cuando así lo aprueben la mayoría de sus Comisionados **(votación y órgano competente)**, podrá ejercer la atracción en cualquier momento, en tanto no haya sido resuelto el recurso de revisión por el organismo garante competente **(temporalidad)**, para lo cual notificará a las partes y requerirá el Expediente al organismo garante correspondiente **(procedimiento)**, o

II. Ejercicio por petición: Cuando la petición de atracción sea formulada por el organismo garante de la Entidad Federativa, éste contará con un plazo no mayor a cinco días, salvo lo dispuesto en el último párrafo del artículo 105 de esta Ley, para solicitar al Instituto que analice y, en su caso, ejerza la facultad de atracción sobre el asunto puesto a su consideración **(plazo de solicitud)**.

PRECLUSIÓN DEL DERECHO DEL GARANTE DE SOLICITAR LA ATRACCIÓN

Transcurrido dicho plazo se tendrá por precluido el derecho del organismo garante respectivo para hacer la solicitud de atracción.

PLAZO PARA RESOLVER SOBRE LA ATRACCIÓN

El Instituto contará con un plazo no mayor a diez días para determinar si ejerce la facultad de atracción, en cuyo caso, notificará a las partes y solicitará el Expediente del recurso de revisión respectivo.

EFECTOS DE LA SOLICITUD DE ATRACCIÓN (TEMPORALIDAD)

Artículo 135. La solicitud de atracción del recurso de revisión interrumpirá el plazo que tienen los Organismos garantes para resolverlo. El cómputo continuará a partir del día siguiente al día en que el Instituto haya notificado la determinación de no atraer el recurso de revisión.

AGOTAMIENTO DEL FONDO EN CASOS DE ATRACCIÓN POR PETICIÓN DEL GARANTE

Artículo 136. Previo a la decisión del Instituto sobre el ejercicio de la facultad de atracción a que se refiere el artículo anterior, el organismo garante de la Entidad Federativa a quien corresponda el conocimiento originario del asunto, deberá agotar el análisis de

todos los aspectos cuyo estudio sea previo al fondo del asunto, hecha excepción del caso en que los aspectos de importancia y trascendencia deriven de la procedencia del recurso.

ESTUDIO DE FONDO DEL RECURSO ATRAÍDO

Si el Pleno del Instituto, cuando así lo apruebe la mayoría de sus Comisionados, decide ejercer la facultad de atracción se avocará al conocimiento o estudio de fondo del asunto materia del recurso de revisión atraído.

NO HAY IMPEDIMENTO POR VOTAR CONTRA LA ATRACCIÓN

El o los Comisionados que en su momento hubiesen votado en contra de ejercer la facultad de atracción, no estarán impedidos para pronunciarse respecto del fondo del asunto.

EFECTOS DE LA RESOLUCIÓN

Artículo 137. La resolución del Instituto será definitiva e inatacable para el organismo garante y para el sujeto obligado de que se trate.

PROCEDENCIA DE LA VÍA DE AMPARO

En todo momento, los particulares podrán impugnar las resoluciones del Instituto ante el Poder Judicial de la Federación.

RECURSO DE REVISIÓN EN MATERIA DE SEGURIDAD NACIONAL

Artículo 138. Únicamente el Consejero Jurídico del Gobierno podrá interponer recurso de revisión en materia de seguridad nacional ante la Suprema Corte de Justicia de la Nación, en el caso que las resoluciones del Instituto a los recursos descritos en este Título, puedan poner en peligro la seguridad nacional.

Dicho recurso de revisión en materia de seguridad nacional se tramitará en los términos que se establecen en el siguiente Capítulo V denominado “Del Recurso de Revisión en materia de Seguridad Nacional,” del presente Título.

CAPÍTULO V
DEL RECURSO DE REVISIÓN EN MATERIA DE SEGURIDAD NACIONAL

INSTANCIA COMPETENTE

Artículo 139. El Consejero Jurídico del Gobierno Federal podrá interponer recurso de revisión en materia de seguridad nacional directamente ante la Suprema Corte de Justicia de la Nación, cuando considere que las resoluciones emitidas por el Instituto ponen en peligro la seguridad nacional.

PLAZO DE INTERPOSICIÓN

El recurso deberá interponerse durante los siete días siguientes a aquél en el que el organismo garante notifique la resolución al sujeto obligado. La Suprema Corte de Justicia de la Nación determinará, de inmediato, en su caso, la suspensión de la ejecución de la resolución y dentro de los cinco días siguientes a la interposición del recurso resolverá sobre su admisión o improcedencia.

CONTENIDO DEL ESCRITO DEL RECURSO

Artículo 140. En el escrito del recurso, el Consejero Jurídico del Gobierno Federal deberá señalar la resolución que se impugna, los fundamentos y motivos por los cuales considera que se pone en peligro la seguridad nacional, así como los elementos de prueba necesarios.

MANEJO DE POR LOS MINISTROS DE INFORMACIÓN RESERVADA

Artículo 141. La información reservada o confidencial que, en su caso, sea solicitada por la Suprema Corte de Justicia de la Nación por resultar indispensable para resolver el asunto, deberá ser mantenida con ese carácter y no estará disponible en el Expediente, salvo en las excepciones previstas en el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública.

MANEJO DE POR LOS MINISTROS DE INFORMACIÓN RESERVADA (CONT.)

En todo momento, los Ministros deberán tener acceso a la información clasificada para determinar su naturaleza, según se requiera. El acceso se dará de conformidad con la normatividad previamente establecida para el resguardo o salvaguarda de la información por parte de los sujetos obligados.

PLENITUD DE JURISDICCIÓN

Artículo 142. La Suprema Corte de Justicia de la Nación resolverá con plenitud de jurisdicción, y en ningún caso, procederá el reenvío (no procede el reenvío).

CONFIRMACIÓN DE LA RESOLUCIÓN

Artículo 143. Si la Suprema Corte de Justicia de la Nación confirma el sentido de la resolución recurrida, el sujeto obligado deberá dar cumplimiento en los términos que establece la disposición correspondiente de esta Ley.

REVOCACIÓN DE LA RESOLUCIÓN

En caso de que se revoque la resolución, el Instituto deberá actuar en los términos que ordene la Suprema Corte de Justicia de la Nación.

CAPÍTULO VI
DE LOS CRITERIOS DE INTERPRETACIÓN

CRITERIOS DE INTERPRETACIÓN

Artículo 144. Una vez que hayan causado ejecutoria las resoluciones dictadas con motivo de los recursos que se sometan a su competencia, el Instituto podrá emitir los criterios de interpretación que estime pertinentes y que deriven de lo resuelto en los mismos, conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

POR REITERACIÓN

El Instituto podrá emitir criterios de carácter orientador para los Organismos garantes, que se establecerán por reiteración al resolver tres casos análogos de manera consecutiva en el mismo sentido, por al menos dos terceras partes del Pleno del Instituto, derivados de resoluciones que hayan causado estado **(requerimiento de votación)**.

COMPOSICIÓN DEL CRITERIO DE INTERPRETACIÓN

Artículo 145. Los criterios se compondrán de un rubro, un texto y el precedente o precedentes que, en su caso, hayan originado su emisión.

IDENTIFICACIÓN

Todo criterio que emita el Instituto deberá contener una clave de control para su debida identificación.

TÍTULO DÉCIMO
FACULTAD DE VERIFICACIÓN DEL INSTITUTO Y LOS ORGANISMOS GARANTES

En este título, se establece el procedimiento de verificación, las autoridades deben usarlo para establecer si los sujetos obligados de resguardar datos personales cumplen con las obligaciones e implementan las medidas de seguridad que les impone la Ley. En el artículo 146, se establece la facultad que tienen el Instituto y los garantes locales de llevarla a cabo, la misma no admite negativa alguna y debe ser confidencial. El numeral 147 establece dos formas para iniciar la verificación: de oficio, cuando la autoridad tenga indicios de que permitan presuponer justificadamente la existencia a violaciones en la ley y, a instancia de parte, cuando existe una denuncia de parte de un titular de datos personales que se considera afectado. El derecho del afectado a denunciar tiene vigencia de un año y no procede en los supuestos de procedencia del recurso de revisión o de inconformidad.

Las denuncias deben cumplir con los siguientes requisitos: nombre, domicilio, hechos, responsable denunciado, firma del denunciante, forma de presentación (escrito libre, formatos, medios electrónicos u otros). Se presentan ante el instituto o los garantes locales y éstos deben dar acuse de recibo. El inicio del procedimiento se da por medio de orden escrita del instituto o garante que declare procedente la denuncia, en esta también se pide documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas (artículos 148 y 149).

En el artículo 149, se establecen también los requisitos que debe cumplir la resolución que ordene la verificación de datos personales en el rubro de la seguridad nacional y pública. En general, el procedimiento de verificación debe contar con una duración máxima de cincuenta días y se podrán ordenar medidas cautelares correctivas y temporales si al hacer la verificación se corre el riesgo de causar un daño o si el daño que se pueda causar es irreparable.

En el artículo 150, se prevé que la verificación concluye con una resolución del instituto o garante local y en la misma se establecerán medidas a adoptar por el responsable; éstos podrán someterse de forma voluntarias a auditorias para determinar si se cumplieron a cabalidad las medidas recomendadas.

CAPÍTULO ÚNICO
DEL PROCEDIMIENTO DE VERIFICACIÓN

FACULTAD DE VERIFICACIÓN

Artículo 146. El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias **(órganos que la ejercen)**, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta.

CONFIDENCIALIDAD EN LA VERIFICACIÓN

En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los Organismos garantes estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.

LA VERIFICACIÓN NO ADMITE NEGATIVA

El responsable no podrá negar el acceso a la documentación solicitada con motivo de una verificación, o a sus bases de datos personales, ni podrá invocar la reserva o la confidencialidad de la información.

FORMAS DE INICIAR LA VERIFICACIÓN

Artículo 147. La verificación podrá iniciarse:

I. De oficio: De oficio cuando el Instituto o los Organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, o

II. A instancia de parte: Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la

presente Ley y demás normativa aplicable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia.

PRECLUSIÓN DEL DERECHO A DENUNCIAR

El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma. Cuando los hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado.

EXCEPCIÓN A LA VERIFICACIÓN

La verificación no procederá en los supuestos de procedencia del recurso de revisión o inconformidad previstos en la presente Ley.

INADMISIBILIDAD DE LA VERIFICACIÓN

La verificación no se admitirá en los supuestos de procedencia del recurso de revisión o inconformidad, previstos en la presente Ley.

INVESTIGACIONES PREVIAS

Previo a la verificación respectiva, el Instituto o los Organismos garantes podrán desarrollar investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respectivo.

REQUISITOS DE LA DENUNCIA

Artículo 148. Para la presentación de una denuncia no podrán solicitarse mayores requisitos que los que a continuación se describen:

I. Nombre: El nombre de la persona que denuncia, o en su caso, de su representante;

II. Domicilio: El domicilio o medio para recibir notificaciones de la persona que denuncia;

III. Hechos: La relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho;

IV. Responsable denunciado: El responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación;

V. Firma del denunciante: La firma del denunciante, o en su caso, de su

representante. En caso de no saber firmar, bastará la huella digital.

FORMA DE PRESENTACIÓN

La denuncia podrá presentarse por escrito libre, o a través de los formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto o los Organismos garantes, según corresponda.

RECEPCIÓN Y TRÁMITE

Una vez recibida la denuncia, el Instituto y los Organismos garantes, según corresponda, deberán acusar recibo de la misma. El acuerdo correspondiente se notificará al denunciante.

INICIO DEL PROCEDIMIENTO

Artículo 149. La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los Organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.

VERIFICACIÓN EN SEGURIDAD NACIONAL Y PÚBLICA. REQUISITOS DE LA RESOLUCIÓN

Para la verificación en instancias de seguridad nacional y seguridad pública, se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados, o de los integrantes de los Organismos garantes de las Entidades Federativas, según corresponda; así como de una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 150.

DURACIÓN

El procedimiento de verificación deberá tener una duración máxima de cincuenta días.

MEDIDAS CAUTELARES

El Instituto o los organismos garantes podrán ordenar medidas cautelares, si del

desahogo de la verificación advierten un daño inminente o irreparable en materia de protección de datos personales, siempre y cuando no impidan el cumplimiento de las funciones ni el aseguramiento de bases de datos de los sujetos obligados.

FINALIDAD DE LAS MEDIDAS CAUTELARES

Estas medidas sólo podrán tener una finalidad correctiva y será temporal hasta entonces los sujetos obligados lleven a cabo las recomendaciones hechas por el Instituto o los Organismos garantes según corresponda.

CONCLUSIÓN DE LA VERIFICACIÓN

Artículo 150. El procedimiento de verificación concluirá con la resolución que emita el Instituto o los Organismos garantes, en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.

SOMETIMIENTO VOLUNTARIO A AUDITORES

Artículo 151. Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto o los Organismos garantes, según corresponda, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.

CONTENIDOS DEL INFORME DE AUDITORÍAS

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.

TÍTULO DÉCIMO PRIMERO
MEDIDAS DE APREMIO Y RESPONSABILIDADES

El último título de esta Ley establece las medidas de apremio y sanciones. Las primeras son las facultades de aplicar la Ley por medios que insinúen el uso de la fuerza e ir en contra de la voluntad de los sujetos de la Ley (y, por lo tanto, son coercitivas). Las segundas son castigos que se dan al incumplimiento de la Ley (coactivas). Es decir, la coerción implica persuadir a alguien a hacer algo por medio del posible uso de la fuerza, mientras que la coacción es usar fuerza para hacer que alguien haga algo que no quiere.

El artículo 152 de esta ley se remite al Capítulo VI del Título Octavo de la Ley General de Transparencia y Acceso a la Información Pública. En éste, su artículo 201 establece que sólo los órganos garantes pueden imponer y ejecutar estos medios (Artículo 201) y bajo reglas muy específicas, como lo son el principio de legalidad contenido en el artículo 14 de la Constitución en lo que respecta a las formalidades esenciales del procedimiento, el 16, que habla de fundamentación y motivación y los principios del derecho penal, que aplican por analogía al derecho administrativo sancionador.

El artículo 201 de la LGTAIP señala que el sujeto de la sanción es el "servidor público encargado de cumplir con la resolución, o a los miembros de los sindicatos, partidos políticos o a la persona física o moral responsable"; es decir, la sanción se aplica al funcionario, no al órgano del que forma parte. Los tipos de apremio son la amonestación pública y multa (aunque existe también la posibilidad de que el INAI o los garantes denuncien posibles hechos delictivos) y el incumplimiento debe difundirse en los portales de obligaciones de transparencia de los garantes (artículo 153).

El artículo 154 establece que, si al aplicar las medidas de apremio aun no estuviera cumplida la resolución, se puede pedir al superior jerárquico (la Ley lo llama requerimiento) que obligue al sujeto sancionado a cumplir. Si se sigue sin cumplir, se aplica el apremio al superior y posteriormente, las sanciones correspondientes. En el

artículo 155, se establece que el Instituto y los organismos garantes son autoridad competente para aplicar el apremio y en la ejecución de las multas, se estará al Servicio de Administración Tributaria o las Secretarías de Finanzas de las Entidades Federativas (artículo 156).

En el artículo 157, se establecen los criterios de aplicación del apremio, en los que se deben considerar la gravedad de la falta, la condición económica y la reincidencia, asimismo, el Instituto y los garantes locales pueden crear lineamientos en la materia. En el artículo 158, se establece la multa agravada por reincidencia y se define a quien incurre en este tipo de conductas. En el artículo 159, se delimita el plazo para implementar las medidas de apremio; en el 160, las autoridades que imponen y aplican la amonestación pública y en el 161, el requerimiento de información necesario para que las autoridades puedan establecer la multa. Contra los medios de apremio procede el recurso ante el Poder Judicial federal o local (artículo 162).

El artículo 163 señala las causales de sanción por incumplimiento, las cuales son actuar con negligencia, dolo o mala fe en la sustanciación del ejercicio de derechos ARCO, el incumplimiento de los plazos de atención, el uso indebido de datos personales, el tratamiento intencional en contravención de los principios y deberes de Ley; no contar con aviso de privacidad, clasificar como confidencial, con dolo o negligencia, datos personales, incumplir el deber de confidencialidad, no establecer las medidas de seguridad, presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad; llevar a cabo la transferencia de datos personales, en contravención a la Ley, obstruir los actos de verificación de la autoridad, crear bases de datos personales, no acatar las resoluciones emitidas por el Instituto y los Organismos garantes, omitir la entrega del informe anual y demás informes. También se establecen las causales de sanción grave, las sanciones no pueden cubrirse con recursos públicos.

El artículo 165 establece que la responsabilidad administrativa es diferente e independiente de la penal y la civil; también se señalan las sanciones para fideicomisos, sindicatos y otros particulares. En el 166, se establece que en el incumplimiento en partidos políticos se debe dar vita al Instituto Nacional Electoral o a los organismos públicos locales electorales de las entidades federativas (en la práctica llamados OPLE). En el caso del Incumplimiento en fideicomisos y fondos públicos, se debe dar aviso (en la Ley se dice “dar vista”) al órgano interno de control.

En el artículo 167, se establece el procedimiento para sancionar a los sujetos que tengan la calidad de servidores públicos y su denuncia por una posible responsabilidad administrativa y por la presunta comisión de un delito.

CAPÍTULO I
DE LAS MEDIDAS DE APREMIO

FUENTE DE LAS MEDIDAS DE APREMIO

Artículo 152. Para el cumplimiento de las resoluciones emitidas por el Instituto o los Organismos garantes, según corresponda, éstos organismos y el responsable, en su caso, deberán observar lo dispuesto en el Capítulo VI del Título Octavo de la Ley General de Transparencia y Acceso a la Información Pública.

TIPOS DE APREMIO

Artículo 153. El Instituto y los Organismos garantes podrán imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

I. Amonestación pública: La amonestación pública, o

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

PUBLICACIÓN DEL INCUMPLIMIENTO

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

PROBABLE RESPONSABILIDAD PENAL

En caso de que el incumplimiento de las determinaciones del Instituto y los Organismos garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163 de la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos **(límite al pago de sanciones)**.

REQUERIMIENTO AL SUPERIOR

Artículo 154. Si a pesar de la ejecución de las medidas de apremio previstas en el artículo anterior no se cumpliere con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora.

APLICACIÓN DEL APREMIO

De persistir el incumplimiento, se aplicarán sobre aquéllas medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista la autoridad competente en materia de responsabilidades.

AUTORIDAD COMPETENTE PARA APLICAR EL APREMIO

Artículo 155. Las medidas de apremio a que se refiere el presente Capítulo, deberán ser aplicadas por el Instituto y los Organismos garantes, por sí mismos o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.

EJECUCIÓN DE LAS MULTAS

Artículo 156. Las multas que fijen el Instituto y los Organismos garantes se harán efectivas por el Servicio de Administración Tributaria o las Secretarías de Finanzas de las Entidades Federativas **(autoridad competente)**, según corresponda, a través de los procedimientos que las leyes establezcan **(procedimiento)**.

CRITERIO DE APLICACIÓN DEL APREMIO

Artículo 157. Para calificar las medidas de apremio establecidas en el presente Capítulo, el Instituto y los Organismos garantes deberán considerar:

I. Gravedad de la falta: La gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto o los Organismos garantes y la afectación al ejercicio de sus atribuciones **(elementos)**;

II. Condición económica del infractor: La condición económica del infractor, y

III. Reincidencia: La reincidencia.

LINEAMIENTOS EN LA MATERIA

El Instituto y los Organismos garantes **(autoridades emisoras)** establecerán mediante

lineamientos de carácter general, las atribuciones de las áreas encargadas de calificar la gravedad de la falta de observancia a sus determinaciones y de la notificación y ejecución de las medidas de apremio que apliquen e implementen, conforme a los elementos desarrollados en este Capítulo.

REINCIDENCIA. MULTA

Artículo 158. En caso de reincidencia, el Instituto o los Organismos garantes podrán imponer una multa equivalente hasta el doble de la que se hubiera determinado por el Instituto o los Organismos garantes.

DEFINICIÓN DE REINCIDENTE

Se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.

PLAZO PARA IMPLEMENTAR LAS MEDIDAS DE APREMIO

Artículo 159. Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.

AMONESTACIÓN PÚBLICA. QUIEN LA IMPONE Y QUIEN LA APLICA

Artículo 160. La amonestación pública será impuesta por el Instituto o los Organismos garantes y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.

REQUERIMIENTO DE INFORMACIÓN PARA ESTABLECER LA MULTA

Artículo 161. El Instituto o los Organismos garantes podrán requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base a los elementos que se tengan a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de Internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto o los Organismos garantes para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

RECURSO CONTRA APREMIO

Artículo 162. En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante el Poder Judicial de la Federación, o en su caso ante el Poder Judicial correspondiente en las Entidades Federativas.

CAPÍTULO II
DE LAS SANCIONES

CAUSALES DE SANCIÓN

Artículo 163. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

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

II. Incumplimiento de los plazos de atención: 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. Uso indebido de datos personales: 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. Tratamiento intencional en contravención de los principios y deberes de Ley: 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 aviso de privacidad: 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: 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: Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley;

VIII. No establecer las medidas de seguridad: 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: 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 la Ley: 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: Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales: 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 los Organismos garantes: No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y

XIV. Omitir la entrega del informe anual y demás informes: 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.

CAUSALES DE SANCIÓN GRAVE

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

SANCIÓN A INTEGRANTES DE PARTIDO POLÍTICO

En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.

PAGO DE SANCIONES. LÍMITE

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

VISTA A LA AUTORIDAD COMPETENTE

Artículo 164. Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que imponga o ejecute la sanción.

INDEPENDENCIA DE LA RESPONSABILIDAD ADMINISTRATIVA DE OTRAS

Artículo 165. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 163 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

DETERMINACIÓN DE OTRAS RESPONSABILIDADES

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

DENUNCIA POR RESPONSABILIDAD

Para tales efectos, el Instituto o los organismos garantes podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

INCUMPLIMIENTO EN PARTIDOS POLÍTICOS

Artículo 166. Ante incumplimientos por parte de los partidos políticos, el Instituto u organismo garante competente, dará vista, según corresponda, al Instituto Nacional Electoral o a los organismos públicos locales electorales de las Entidades Federativas competentes, para que resuelvan lo conducente, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.

INCUMPLIMIENTO EN FIDEICOMISOS Y FONDOS PÚBLICOS

En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto u organismo garante competente deberá dar vista al órgano interno de control del sujeto obligado relacionado con éstos, cuando sean servidores públicos, con el fin de que instrumenten los procedimientos administrativos a que haya lugar.

INFRACCIONES POR SERVIDORES PÚBLICOS

Artículo 167. En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto o el organismo garante, deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un Expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.

CONDUCCIÓN DEL PROCEDIMIENTO

La autoridad que conozca del asunto, deberá informar de la conclusión del procedimiento y, en su caso, de la ejecución de la sanción al Instituto o al organismo garante, según corresponda.

DENUNCIA POR POSIBLE RESPONSABILIDAD

A efecto de sustanciar el procedimiento citado en este artículo, el Instituto, o el organismo garante que corresponda **(órgano que la elabora)**, deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente **(órgano que la recibe)**, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad **(contenido de la denuncia)**.

EXPEDIENTE

Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

PLAZO DE ENVÍO

La denuncia y el Expediente deberán remitirse a la contraloría, órgano interno de control o equivalente dentro de los quince días siguientes a partir de que el Instituto o el organismo garante correspondiente tenga conocimiento de los hechos.

DENUNCIA POR LA PRESUNTA COMISIÓN DE UN DELITO

Artículo 168. En caso de que el incumplimiento de las determinaciones de los Organismos garantes implique la presunta comisión de un delito, el organismo garante respectivo deberá denunciar los hechos ante la autoridad competente.

Roberto Mancilla es Presidente de la Comisión Nacional de Transparencia de Movimiento Ciudadano. Es Licenciado en Derecho por Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey y Doctor en Derecho por la Universidad de California, Berkeley. Le gusta escribir cuentos cortos y hacer artículos académicos.