

INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE EXPIDE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS QUE PRESENTAN LAS Y LOS SENADORES LAURA ANGÉLICA ROJAS HERNÁNDEZ, ALEJANDRO DE JESÚS ENCINAS RODRÍGUEZ, MARÍA CRISTINA DÍAZ SALAZAR, HÉCTOR LARIOS CÓRDOVA, FERNANDO YUNES MÁRQUEZ, MARCELA TORRES PEIMBERT, ZOÉ ROBLEDO ABURTO, ARMANDO RÍOS PITER, ISIDRO PEDRAZA CHÁVEZ Y PABLO ESCUDERO MORALES, INTEGRANTES DE LOS GRUPOS PARLAMENTARIOS DEL PARTIDO ACCIÓN NACIONAL, DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL, DEL PARTIDO DE LA REVOLUCIÓN DEMOCRÁTICA Y DEL PARTIDO VERDE ECOLOGISTA DE MÉXICO DEL SENADO DE LA REPÚBLICA.

Las y los Senadores Laura Angélica Rojas Hernández, Alejandro de Jesús Encinas Rodríguez, María Cristina Díaz Salazar, Héctor Larios Córdova, Fernando Yunes Márquez, Marcela Torres Peimbert, Zoé Robledo Aburto, Armando Ríos Piter, Isidro Pedraza Chávez y Pablo Escudero Morales, integrantes de los Grupos Parlamentarios del Partido Acción Nacional, Partido Revolucionario Institucional, Partido de la Revolución Democrática y del Partido Verde Ecologista de México del Senado de la República, con fundamento en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos, y conforme a lo dispuesto por los artículos 8, numeral 1, fracción I; 163 y 164 del Reglamento del Senado de la República, presentamos a la consideración del Pleno iniciativa con proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados con arreglo a la siguiente:

EXPOSICIÓN DE MOTIVOS

**Ley General de Protección de Datos Personales en
Posesión de Sujetos Obligados**

Concepto

El concepto del derecho fundamental a la protección de datos personales se entiende como el poder de disposición que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.¹

¹ Al respecto puede consultarse la resolución STC 292/2000 del Tribunal Constitucional español.

En tanto, la privacidad es concebida como el derecho a ser dejado solo, el derecho a no ser molestado, a no ser que medie orden o mandato de autoridad competente que funde y motive el acto de molestia.²

Por su parte, la intimidad puede concebirse como el ámbito donde el individuo ejerce plenamente su autonomía personal, el reducto último de la personalidad, ahí donde una persona es lo que es.³

Conforme a lo señalado, el derecho a la protección de datos personales es un derecho fundamental autónomo y distinto al resto de los derechos fundamentales que si bien puede guardar una cercana relación con derechos como el de privacidad e intimidad, posee características propias y por tanto tiene objetivos e implicaciones diversas.

En particular, el derecho de protección de datos personales está asociado a la evolución tecnológica que vivimos en nuestros días, en la que el flujo de información personal es incuantificable. Así, fue necesaria la generación de un nuevo derecho a la protección de datos personales o a la autodeterminación informativa que respondiera de manera efectiva a los retos que el uso de los datos personales implicó en el contexto de los desarrollos tecnológicos modernos.

En ese orden de ideas, el derecho a la protección de datos personales se configuró como una herramienta cuyo objetivo era restituir a las personas el control sobre su información personal, control que se diluyó hasta prácticamente perderse a partir del nacimiento de los desarrollos tecnológicos, particularmente aquellos que se dieron en el campo de la informática.

Precisamente es en el derecho a la protección de datos personales en donde podemos encontrar las respuestas ante los retos que ha ido planteando el avance del desarrollo tecnológico, herramientas como el derecho al olvido (derecho de cancelación) han ido equilibrando los intereses en presencia de situaciones como las descritas. Así ante esa memoria indeleble que pueden significar diversas plataformas en Internet, ahora es posible ejercer un derecho al olvido que permite eliminar de las mismas, cualquier información que le pertenezca a una persona y de ese modo garantizar el poder de disposición sobre la información personal.

En el espacio de la Unión Europea, se desarrolló y delineó, como hoy lo conocemos, el derecho fundamental a la protección de los datos personales con la finalidad de dotar a las personas de un instrumento idóneo que les permitiera hacer frente a los efectos producidos por los desarrollos informáticos en el tratamiento de los datos personales.

México en su interacción con otras naciones, concretamente a través de su integración en la Red Iberoamericana de Protección de Datos, trabajó intensamente para incorporar en su marco normativo este necesario derecho humano.

² Este concepto de privacidad corresponde con lo previsto en el diversos instrumentos internacionales de derechos humanos como el artículo 12 de la Declaración Universal de los Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos y 7 de la Carta de los Derechos Fundamentales de la Unión Europea.

³ Fuente: Garzón Valdés, Ernesto, *Lo íntimo, lo privado y lo público*, México, IFAI, 2005, Cuadernos de Transparencia 06, p. 16. Disponible en: <http://inicio.ifai.org.mx/Publicaciones/cuadernillo6.pdf>.

Evolución del marco jurídico en México

El 7 de febrero de 2014 se publicó en el Diario Oficial de la Federación el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia. Esta iniciativa que se presenta, tiene el objeto de conformar la legislación secundaria que desarrolla el contenido del derecho a la protección de datos personales que reconoce nuestra Carta Magna en dicha reforma.

Desde el 2002, con la expedición de la Ley Federal de Transparencia, se incorporó el derecho a la protección de datos personales en el marco jurídico mexicano, como límite o contrapeso al derecho de acceso a la información en la transparencia, con algunas escasas menciones a lo largo del articulado. En esa ley, la protección de datos personales todavía era insoslayable y dependiente del derecho de acceso a la información y no contaba con el carácter de un derecho autónomo.

Fue hasta el año 2005 que se publicaron en el Diario Oficial de la Federación los Lineamientos de Protección de Datos Personales, los cuales representan una regulación sin precedentes en México al ser primer instrumento normativo,⁴ estrictamente en materia de protección de datos personales, que desarrolla aspectos sustantivos en la materia tales como principios, deberes y derechos.

A partir de 2006, en el contexto de la reforma al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia y acceso a la información, se hace la primera referencia constitucional al derecho a la protección de datos personales, pero sin regularlo sustancialmente, reiterando el papel de este derecho como contrapeso del derecho de acceso a la información.

Debido a la estrecha relación que existe entre el derecho a la privacidad y a la intimidad con el derecho de protección de datos personales, este derecho se dotó de contenido, tres años después, con una adición de un párrafo segundo al artículo 16 constitucional en el que se establece que:

“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”.

Con lo anterior, se deja manifiesto que el derecho de protección de datos personales es un derecho distinto y autónomo de otros derechos humanos.

⁴ Se trata de un instrumento muy relevante históricamente con la desventaja de ser un lineamiento de carácter administrativo (no ley ni reglamento) y que únicamente es aplicable a las dependencias y entidades de la Administración Pública Federal.

Conjuntamente con la reforma al citado artículo 16 constitucional, se adiciona la fracción XXIX-O del artículo 73, en donde se establece como facultad exclusiva del Congreso de la Unión, legislar en materia de protección de datos personales en posesión de los particulares. Con ello, esta materia se constituye como materia federal, no concurrente, por lo que las entidades federativas no cuentan con facultades para legislar al respecto.

Así, en 2010 se expidió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares cuyo objeto es la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Esta ley encomendó al Instituto Federal de Acceso a la Información y Protección de Datos constituirse en el garante de este derecho.

No obstante el avance de la materia con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la reciente reforma de 2014 en materia de transparencia reconoce la necesidad de abundar en el derecho de protección de datos personales en posesión de sujetos obligados.

El marco jurídico de la protección de datos en posesión de sujetos obligados ha resultado insuficiente. Desde la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en 2003, hasta el 31 de diciembre de 2013, el Instituto Federal de Acceso a la Información y Protección de Datos, recibió 7,297 recursos de revisión presentados en contra de solicitudes en materia de acceso y corrección de datos personales en posesión de las dependencias y entidades federales, las cuales de 2003 al 2013, ascendieron a la cantidad de 192, 453.

Las tres entidades que recibieron más solicitudes de acceso y corrección de datos personales en 2013 fueron: el IMSS, con 25,726 solicitudes; el ISSSTE, con 3,387, y el Instituto Nacional de Cardiología Ignacio Chávez, con 293. En el IMSS, 44.3 por ciento involucraban información sobre expedientes médicos, 25.3 por ciento de las solicitudes de acceso a datos personales correspondieron a pensiones o jubilaciones y 21.6 por ciento se refirieron a semanas cotizadas por los derechohabientes. De igual forma, en el caso del ISSSTE, 50.5 por ciento de los requerimientos fueron sobre expedientes médicos, 14.3 por ciento buscaban información relacionada con pensiones o jubilaciones y 8.8 por ciento acerca de afiliaciones. También en el Instituto Nacional de Cardiología Ignacio Chávez, la solicitud más frecuente fue la de expedientes médicos, con 93.8 por ciento⁵. En el Cuadro 1.2 se enlistan las 20 dependencias y entidades con mayor número de solicitudes de acceso y corrección de datos personales, con la cantidad de solicitudes anuales que recibieron de 2003 a 2013, así como el total acumulado a diciembre de 2013.

De 2007 a 2012, el IFAI llevó a cabo las primeras verificaciones con el propósito fundamental de establecer un esquema que permitiera, en su calidad de órgano garante, revisar el cumplimiento de las normas respectivas de oficio y de esta manera generar una política preventiva y no sólo reactiva.

⁵ La clasificación se realizó con base en una muestra representativa de la totalidad de las solicitudes de información ingresadas a cada una de las dependencias y entidades.

Entre las dependencias y entidades federales verificadas destacan la Secretaría de Gobernación, Secretaría de Relaciones Exteriores, Secretaría de Seguridad Pública, Secretaría de Hacienda y Crédito Público, Secretaría de Salud, Secretaría de Desarrollo Social y el Instituto Mexicano del Seguro Social, entre otras. Estas verificaciones concluyeron en 2012.

No resulta menor, por tanto, esta posibilidad histórica que brinda el constituyente permanente de dotar a los habitantes del territorio mexicano de una ley general de protección de datos personales para el ámbito público, que desarrolle sustantivamente este derecho a partir de los principios, deberes y derechos que internacionalmente han sido reconocidos, de manera que la protección de datos personales se vea emancipada del derecho de acceso a la información, y en ese sentido deje de visualizarse como un accesorio de ese derecho. A partir de esta consideración, el derecho a la protección de datos deberá considerarse en un esquema de igualdad con el acceso a la información y el resto de los derechos fundamentales que establece nuestra Carta Magna.

La reforma en materia de transparencia, sin duda marcó un hito en el desarrollo del derecho a la protección de datos en México, ya que a través de la misma se establecen las bases constitucionales para dotar al sector público federal de un régimen legal en materia de protección de datos, más aun, se abre la posibilidad de que se emita una ley general en la que se establezcan los principios, bases y procedimientos que de manera uniforme regule este derecho en nuestro país en los tres niveles de gobierno.

Estas modificaciones constitucionales poseen un matiz histórico en materia de datos personales, pues, por una parte, dota al IFAI de autonomía constitucional y lo sitúa como el máximo órgano garante en materia de protección de datos personales en el ámbito público federal y, por otra, fija las bases para la creación de una ley general de protección de datos personales que permitirá dimensionar, en una situación sin precedentes, en toda su extensión el derecho a la protección de datos personales entre los entes públicos de los tres órdenes de gobierno.

El decreto de la reforma constitucional establece en su artículo segundo transitorio el mandato al Congreso de la Unión para "expedir la Ley General del Artículo 6º. de esta Constitución" en relación con el artículo 73, fracción XXIX-S que establece la obligación para "expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno".

Con esta propuesta, se busca que México dote a sus habitantes de leyes de vanguardia en el espacio de los derechos fundamentales con el objeto de proveerles de herramientas jurídicas que les permitan imponer un límite a las actuaciones de las autoridades que pudieran conculcar la esfera de derechos de los particulares. En este caso específico, un límite para ejercer de manera plena el derecho a la autodeterminación informativa de manera que cada persona en este país decida libremente sobre el uso y destino de sus datos personales, teniendo en todo momento el derecho a acceder, rectificar, cancelar y oponerse legítimamente a determinados tratamientos de datos.

En ese orden de ideas, resulta conveniente que las leyes de acceso a la información prevean un apartado de protección de datos personales, para fijar los límites del acceso a la información frente a los datos personales, así como para establecer procedimientos y garantías para los casos de apertura de datos por considerarse de interés público, también lo es que el contenido sustantivo del derecho de protección de datos personales tanto el constitucional, como el que deviene de los tratados internacionales en materia de derechos humanos, de acuerdo al artículo 1 constitucional, sea desarrollado por leyes específicas y especializadas en materia de protección de datos personales.

Bajo la concepción antes descrita es que el presente proyecto ha desarrollado, una ley general de protección de datos personales que de manera independiente y autónoma a cualquier otro derecho, empodere a los titulares del derecho frente al Estado Mexicano para garantizar el control sobre su información personal.

Presentación de la iniciativa

Esta iniciativa que se presenta retoma la iniciativa presentada por el Instituto Federal de Acceso a la Información y Protección de Datos en la Semana de la Transparencia de octubre del año pasado y que hicieron llegar al Senado de la República. El Instituto, así como los organismos garantes, como órgano especializados, en conjunto con la academia y las organizaciones de la sociedad civil, han sido pieza fundamental para la consecución de los objetivos de la reforma constitucional y en la expedición de la legislación secundaria en materia de transparencia.

A dicha iniciativa se le hicieron algunas modificaciones derivadas de las ponencias y las conclusiones de la misma Semana de la Transparencia, así como del evento pasado con motivo del Día Internacional de la Protección de Datos Personales el 28 de enero de 2015; las experiencias compartidas en el XII Encuentro Iberoamericano de Protección de Datos Personales, así como en razón de la armonización, para darle coherencia a la Ley General de Protección de Datos, con relación a la Ley General de Transparencia y Acceso a la Información que aprobamos el pasado 16 de abril y que está pendiente de publicación por parte del Ejecutivo Federal.

En este primer gran esfuerzo de dotar de contenido al derecho de protección de datos personales conforme a la reforma constitucional de febrero de 2014, nos hemos sumado Senadores de las distintas fuerzas políticas de los Grupos Parlamentarios de los Partidos de Acción Nacional, de la Revolución Democrática y del Revolucionario Institucional para conformar una legislación secundaria sólida y de consensos.

La presentación de esta iniciativa responde al mandato constitucional y la apremiante urgencia de la legislación secundaria en la materia, en un decidido empuje al desarrollo del derecho de protección de datos personales.

No obstante, el reto mayúsculo que implica la construcción armónica de un Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, así como la expedición de una ley general en la materia que regule a los tres órdenes de

gobierno, en relación con la relevancia del ejercicio de un derecho humano, en el seno de un grupo plural de legisladores y de expertos en la materia que previamente han expuesto distintas concepciones de legislar este derecho, así como sus mecanismos para hacerlo efectivo, han mantenido vigentes algunos temas de debate en la construcción del modelo de la protección de datos personales.

Por lo anterior, buscaremos que en el periodo de dictamen, en conjunto con los expertos en la materia y de la participación ciudadana, se dilucidan los temas a debate como la procedencia de ciertos deberes de los sujetos obligados, las facultades del órgano garante nacional en materia de protección de datos personales o la aplicación de esta ley a los sindicatos y particulares.

Contenido de la iniciativa

El documento de trabajo relativo a una Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se integra de 144 artículos, 12 títulos, 24 capítulos y 6 artículos transitorios.

El Título I se compone de dos Capítulos. El Capítulo I establece la naturaleza y objeto de la ley, un apartado de definiciones y las excepciones generales al derecho a la protección de datos personales.

Una de las grandes novedades de la reforma constitucional fue la ampliación de los sujetos obligados en materia de protección de datos personales. En tal sentido, conviene hacer algunos apuntes respecto de la ubicación (sector público o privado) que se debe dar a aquellos entes que no constituyen propiamente un órgano del Estado y particularmente referir a los partidos políticos.

Conforme a la Constitución todo ciudadano mexicano tiene la libertad de ejercer su derecho de asociación con fines políticos a través de la conformación o afiliación a un partido político.

Los partidos políticos son entidades de interés público que tienen como fin promover la participación del pueblo en la vida democrática y contribuir a la integración de la representación nacional.

Este atributo que tienen los partidos políticos relacionado con el interés público, no necesariamente debe interpretarse en el sentido de considerar que se está frente a entes estatales o para equipararlos a éstos, independiente de las funciones que realizan en el marco de un país democrático y de las prerrogativas que reciben para realizar dichas funciones.

Los partidos políticos, en su calidad de organizaciones de ciudadanos, hacen posible el acceso de éstos al ejercicio del poder público de acuerdo con los programas, principios e ideas que postulan, mediante el derecho al voto.

La reforma al artículo 6 constitucional refiere como universo de sujetos obligados a cualquier autoridad, entidad, órgano u organismo que forme parte de los Poderes

Ejecutivo, Legislativo y Judicial (con excepción de aquellos asuntos jurisdiccionales que corresponden a la Suprema Corte de Justicia de la Nación), órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal.

Analizado desde la óptica del derecho de acceso a la información, resulta clara la reforma y los objetivos que persigue al sujetar a un régimen de derecho público de transparencia a sujetos no gubernamentales que por el ejercicio de recursos públicos o por la realización de actos de autoridad son equiparables, para efectos de acceso a la información, a entidades integrantes del Estado y por tanto susceptibles de observar el cumplimiento de determinadas obligaciones derivadas del derecho fundamental en cuestión. Lo anterior, resulta totalmente atendible considerando que el ejercicio de recursos públicos, así como la realización de actos de autoridad requieren mantenerse en la esfera de lo público, más allá de la naturaleza pública o privada del sujeto que aplique el recurso o realice el acto, considerando que *per se* se trata de elementos integrantes y fundamentales del actuar público, propiamente de la *res publica*.

En el caso derecho a la protección de datos personales las razones apuntadas para el acceso a la información no resultan necesariamente trasladables, partiendo de la premisa de que se trata de dos derechos distintos con objetivos diversos. En el acceso a la información se busca proveer lo necesario para garantizar el acceso a la información pública y favorecer la rendición de cuentas, en términos generales, mientras que en caso de la protección de datos personales el objetivo es garantizar el poder de disposición que las personas tienen respecto de su información personal.

La integración de los nuevos sujetos obligados no gubernamentales en términos generales se alinea con los objetivos que persigue el derecho de acceso a la información ¿en materia de protección de datos es posible hacer esa misma afirmación?

En ese orden de ideas la reforma constitucional puede ser visualizada desde dos criterios interpretativos relacionados con el régimen de protección de datos personales al cual se deberán constreñir los partidos políticos, sindicatos y demás sujetos obligados no gubernamentales en el tratamiento de datos personales.

El primer criterio se orienta a incluir a los partidos políticos, sindicatos y demás sujetos obligados no gubernamentales en el régimen de protección de datos personales aplicable al sector público, equiparándolos en esta materia a un ente del Estado, con los correspondientes efectos jurídicos. Uno de los cambios esenciales entre un régimen de protección de datos del ámbito público y del privado, radica en el hecho de que las entidades gubernamentales o autoridades no pueden ser objeto de sanciones como institución. Esto es, en caso de acreditarse alguna especie de irregularidad en el tratamiento de datos personales, se ordenaría la restitución en la garantía afectada y, en todo caso, se daría vista a la contraloría o equivalente para que se inicie una investigación tendente a determinar si algún servidor público incurrió en alguna infracción administrativa susceptible de sanción, en cuyo caso se estaría sancionando al servidor público en lo individual y no a la institución estatal.

La segunda postura obedece a realizar una interpretación armónica de los artículos 1 y 16 constitucional con la finalidad de que el régimen de protección de datos personales a los partidos políticos, sindicatos y demás sujetos obligados no gubernamentales sea el que se encuentra previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, porque: (i) se trata de personas que no forman parte del Estado; (ii) atendiendo al principio *pro persona* este régimen resulta más benéfico para los titulares del derecho al contar con herramientas más poderosas, como el régimen de sanciones (multas) para los sujetos regulados, para hacer efectiva la garantía fundamental y (iii) en cumplimiento del principio de interdependencia el ejercicio pleno de este derecho permite, a su vez, el ejercicio de otras garantías fundamentales como la libertad de asociación política o sindical y el derecho al voto, entre otras.

En esa perspectiva, el elemento que no deja lugar a dudas en el texto constitucional es el relativo a que los partidos políticos, sindicatos y demás sujetos obligados no gubernamentales referidos en el decreto de reforma del pasado 7 de febrero, son, a partir de la entrada en vigor del mismo, antes obligados bajo la esfera de competencia del organismo garante a nivel nacional, sea en la esfera pública, en cuyo caso se haría la distribución de competencias entre los tres niveles de gobierno, sea en la esfera privada, en donde de manera exclusiva conocería de los asuntos relacionados con ellos, como ha venido ocurriendo por ejemplo en el caso de los sindicatos.

Teniendo en cuenta las dos perspectivas apuntadas, en cuanto al régimen de protección de datos personales al cual se deberán constreñir los partidos políticos, sindicatos y demás sujetos obligados no gubernamentales en el tratamiento de datos personales, se estima que en el caso de los partidos políticos, como se refleja en el articulado de la propuesta, al actuar en forma similar al Estado, pueden obrar con un doble carácter, como entidades de interés público y como personas morales de derecho privado. En el primer caso, su acción proviene del ejercicio de las facultades de que se hayan investidos como partidos políticos (organización, funciones y prerrogativas) y en la segunda situación, obran en las mismas condiciones que los particulares, esto es, contraen obligaciones y derechos de la misma naturaleza y en la misma forma que los individuos.⁶

En ese sentido, el tratamiento de datos personales que se da en el contexto de la actividad político/electoral de los partidos es en el ejercicio de las facultades de que se encuentran investidos, por lo que la regulación para la utilización de datos personales, en su calidad de entidad de interés público, debe inscribirse en un régimen de derecho público que se alinee con la naturaleza propia de sus actividades (actividades de interés público) y, por la otra, que el órgano garante en materia de datos considere la trascendencia de los partidos en la consolidación de la vida democrática del país al valorar su actuar, como parte de los sujetos regulados del derecho público, sin que se interprete como un espacio en el que sin justificación alguna la materia electoral y la actividad política prevalecen frente a la protección de los datos personales.

En cuanto a sindicatos y demás sujetos obligados no gubernamentales en el tratamiento de datos personales, dado que no comparten las características atribuidas a los partidos

⁶ Séptima época, registro 250931, Tribunales Colegiados de Circuito, tesis aislada, Semanario Judicial de la Federación, volumen 145-150, sexta parte, materia administrativa, página 188.

políticos, de modo que resulten asimilables a los órganos del Estado, se considera que no deben ser objeto de regulación de derecho público, como la que se busca desarrollar a través de la presente propuesta.

Por otra parte, en cuanto a las garantías de que se busca dotar a través de este derecho fundamental, se prevé la imposibilidad de crear sistemas de datos personales sensibles, a manera de regla general.

En cuanto a los límites que puede llegar a enfrentar este derecho se establece la posibilidad de conciliar el derecho a la protección de datos personales con el ejercicio de la libertad de expresión e incluye una cláusula de interpretación conforme. En tal sentido, el documento de trabajo elaborado en el seno de la Comisión de Datos Personales de la Conferencia Mexicana para el Acceso a la Información (COMAIP) resultó un referente de gran utilidad, ya que a partir de sus propuestas se retoma el esquema de equilibrios que una ley de protección de datos debe tener frente al ejercicio de las libertades de información y prensa.

Al respecto, se considera muy relevante fijar un punto de partida legal que sienta las bases para conciliar el derecho a la protección de datos personales y la libertad de expresión que garantiza la Carta Magna en su artículo 6, situación que se alinea con los estándares internacionales en la materia.

Esto permitirá armonizar estos derechos fundamentales desde una base legal y de esa manera se brindará certeza jurídica a las personas sobre los límites que puede llegar a encontrar el derecho a la protección de datos personales. Conforme a la vocación de este tipo de leyes, en este documento de trabajo únicamente se sienta una base general para que la misma pueda ser desarrollada por las legislaturas federal, estatal y por la Asamblea del Distrito Federal atendiendo a las necesidades de cada nivel y espacio de gobierno.

En este Capítulo I destaca el apartado de definiciones, mismo que refleja de manera importante la homologación de los términos previstos en este instrumento a los reconocidos en los Estándares Internacionales sobre Protección de Datos y Privacidad, también conocidos como Resolución de Madrid (en lo sucesivo, Estándares Internacionales o Resolución de Madrid). Se trata de conceptos propios de la terminología del derecho a la protección de datos personales, necesarios para dotar de sentido al derecho mismo y para reconocerle una dinámica propia, distinta de otros derechos.

Si bien algunas definiciones son similares a las reconocidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, otras han sido modificadas y complementadas con elementos adicionales para adecuarlas al contexto del sector público.

Entre las definiciones adoptadas destacan la de datos personales, misma que ha quedado establecida en un sentido amplio para comprender originalmente cualquier información concerniente a una persona física identificada o identificable; igualmente, resalta la definición de datos personales sensibles, concepto que conlleva en la práctica una distinción entre diferentes categorías de datos, los cuales deben ser especialmente protegidos para evitar situaciones y consecuencias no deseadas para los titulares, tales como una afectación a su esfera íntima, discriminación o exposición a un riesgo grave.

Asimismo, en este Capítulo I se reconoce la idea defendida por la doctrina y los Tribunales consistente en que ningún derecho es absoluto. Así, el derecho a la protección de datos personales aparece como un derecho que tiene como límite en cuanto a su observancia y ejercicio la protección de la seguridad nacional, las disposiciones de orden público, la seguridad y salud públicas, o los derechos de terceros. Este elemento, al igual que en el caso de libertad de expresión, deberá ser desarrollado en las leyes federal, estatales y del Distrito Federal, según corresponda, conforme a su competencia y de ese modo cumplir con las formalidades que el artículo 16 constitucional prevé para la aplicación de excepciones a los principios que rigen el tratamiento de los datos y a los derechos que están atribuidos a los titulares de los mismos.

En este punto resulta relevante destacar que si bien se consideraron entre las diversas posibilidades normativas el incluir algún régimen "especial" en materias como las que apunta la Constitución Federal, dicha situación no se estimó pertinente en el ámbito de una ley general al tratarse de situaciones que excepcionalmente deberán presentarse y que deberá ser en las leyes federal, estatales o del Distrito Federal, o bien, en las leyes especiales de cada materia en las que se plasmen las excepciones y alcances a las mismas conforme a las particularidades de cada caso.

En tal sentido, resulta claro que todas las autoridades están obligadas a respetar los principios que rigen todo tratamiento de datos personales con estricto apego a lo que establezca la ley y que únicamente en las situaciones excepcionales que la misma fije podrán actuar en sentido diverso pero, en ambos casos, respetándola de manera irrestricta.

También se estimó importante incluir una referencia al principio del interés superior del menor, de manera que se constituya en el eje rector que oriente las determinaciones de los sujetos regulados para cualquier tratamiento de datos que tenga que ver con menores de edad y adolescentes.

La normativa internacional y nacional reconoce que los menores, por su falta de madurez física y mental, necesitan de protección y cuidados especiales. En el tratamiento de datos personales de menores, el principio jurídico fundamental es el interés superior del niño. El Poder Judicial de la Federación se ha referido en diversas tesis al principio del "interés superior del menor". Este principio consiste en el conjunto de valores, interpretaciones y procesos destinados a garantizar el pleno desarrollo humano integral, así como el máximo bienestar personal, familiar y social de los niños, niñas y adolescentes.

Para mejor referencia se cita el artículo 3 de la Convención sobre los Derechos del Niño:

"Artículo 3

1. En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño.

2. Los Estados Partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y, con ese fin, tomarán todas las medidas legislativas y administrativas adecuadas.”

Así las cosas, el “principio de interés superior del niño” constituye el eje cuya protección deben promover y garantizar los Estados en el ejercicio de sus funciones, por tratarse de un asunto de orden público e interés social.

En el ámbito nacional, la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, que tiene su fundamento en el artículo 4º, párrafo sexto de la Constitución Política de los Estados Unidos Mexicanos, establece en relación con el interés superior del menor:

“**Artículo 3.** La protección de los derechos de niñas, niños y adolescentes, tiene como objetivo asegurarles un desarrollo pleno e integral, lo que implica la oportunidad de formarse física, mental, emocional, social y moralmente en condiciones de igualdad.

Son principios rectores de la protección de los derechos de niñas, niños y adolescentes:

A. El del interés superior de la infancia.
[...”

Artículo 14. Niñas, niños y adolescentes tienen derecho a que se les asegure prioridad en el ejercicio de todos sus derechos, especialmente a que:
[...]

C. Se considere el diseñar y ejecutar las políticas públicas necesarias para la protección de sus derechos.
[...”

Tratándose de menores de edad, el Estado debe ser particularmente sensible ante la injerencia en la vida privada de los menores, a fin de que éstos se desarrollen de forma plena, ya que, por tratarse de personas que todavía no han alcanzado la suficiente madurez física y psicológica, se encuentran en una situación de vulnerabilidad especial.

El principio del “interés superior del niño” debe constituir un eje rector en el diseño y aplicación de políticas públicas.

Respecto a la interpretación en el presente documento de trabajo, se incluye un artículo que integra una cláusula de interpretación conforme a lo previsto en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales que resulten aplicables, siempre y cuando hubieren sido suscritos y ratificados por México, así como la interpretación que de los mismos realicen o hayan realizado la Suprema Corte de Justicia de la Nación y los órganos internacionales cuya jurisdicción sea reconocida por el Estado Mexicano.

Por su parte, el Capítulo II se establecen las bases para el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Se incluyen cuestiones destacables como son el objeto del Sistema y la elaboración de un programa nacional de protección de datos personales que tendrá por objeto, entre otros, coadyuvar en la definición de políticas públicas, estrategias, acciones y metas para promover una cultura del derecho a la protección de datos personales.

El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en este último componente tiene como finalidad coordinar y evaluar las acciones relativas a la política pública transversal en materia de protección de datos personales; garantizar el efectivo ejercicio y respeto del derecho a la protección de datos personales, así como promover la educación y una cultura de protección de datos personales en todo el territorio nacional, para lo cual funcionará con los instrumentos, políticas y acciones que se desarrollen acorde a los principios, bases y prerrogativas que rigen este derecho fundamental.

De este modo, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales será el cauce en el cual confluyan las propuestas, necesidades, ideas, opiniones de la ciudadanía y de los organismos garantes y sobre el cual se construyan los cimientos de este derecho en nuestro país a partir de dos ejes fundamentales: comunicación y coordinación. Comunicación frente a la sociedad para generar conciencia sobre la importancia de proteger y cuidar los datos personales en el contexto del desarrollo tecnológico actual. Comunicación con los sujetos regulados de la norma para el mejor entendimiento y así facilitar la observancia de la ley y coordinación entre organismos garantes para propiciar que cada persona de este país cuente con un derecho efectivo y bajo las mismas garantías, más allá de la autoridad, entidad u órgano que trate los datos personales en cualquiera de los niveles de gobierno.

El modelo del de Transparencia, Acceso a la Información y Protección de Datos Personales es el elemento innovador y la columna vertebral de este documento de trabajo, ya que tiene como objetivo el diseño, la ejecución y evaluación de un programa nacional de protección de datos personales que defina la política pública, y en función de la misma, se desarrollen instrumentos y acciones concretas para:

- Consolidar una cultura de protección de datos personales entre la sociedad mexicana.
- Fomentar el ejercicio del derecho a la protección de datos personales.
- Capacitar a los servidores públicos de los tres niveles de gobierno en este tema.
- Establecer mecanismos que permitan la medición, reporte y verificación de las metas establecidas en el sistema.

Este Título II se compone de dos Capítulos. En el primero se reconocen y desarrollan los principios relativos al tratamiento de los datos personales. A manera de referencia, los Estándares Internacionales resumen los principios del tratamiento en los siguientes:

- **Principio de lealtad y legalidad.** El tratamiento de datos personales deberá realizarse respetando la legislación nacional aplicable y los derechos y libertades de las personas.

- **Principio de consentimiento.** Como regla general, los datos personales sólo podrán ser tratados con el consentimiento de su titular.
- **Principio de finalidad.** El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento.
- **Principio de proporcionalidad.** El tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas.
- **Principio de calidad.** El responsable deberá asegurar en todo momento que los datos personales sean exactos, así como que se mantengan completos y actualizados para el cumplimiento de las finalidades para las que sean tratados. Además, el responsable deberá limitar el periodo de conservación de los datos personales tratados al mínimo necesario.
- **Principio de transparencia.** El responsable deberá facilitar a los titulares, al menos, la información acerca de su identidad, la finalidad para la que pretenda realizar el tratamiento, los destinatarios a los que prevé comunicar los datos personales y el modo en que los titulares podrán ejercer los derechos de acceso, rectificación, cancelación y oposición al tratamiento, así como cualquier otra información necesaria para garantizar el tratamiento leal de los datos de carácter personal.
- **Principio de responsabilidad.** El responsable deberá adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en los Estándares y en la legislación nacional aplicable. También, deberá allegarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión.

En el documento de trabajo relativo a una Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante el documento de trabajo), se reconocieron los siguientes principios: licitud, consentimiento, calidad, finalidad, lealtad, proporcionalidad, información y responsabilidad. Dichos principios constituyen ejes rectores a partir de los cuales se desprenden obligaciones concretas para el responsable del tratamiento y son similares a los previstos en los Estándares Internacionales y a los principios plasmados en el anteproyecto COMAIP.

- **Licitud.** Precisa el deber que tiene el responsable de llevar a cabo el tratamiento de los datos personales conforme a las facultades o atribuciones que la normatividad le confiere.
- **Consentimiento.** Obliga al responsable a obtener el consentimiento del titular de manera libre, específica e informada.
- **Calidad.** Conlleva el deber a cargo del responsable de adoptar medidas necesarias para mantener exactos, correctos y actualizados los datos personales que se encuentren en su posesión.
- **Finalidad.** Construye al responsable a efectuar el tratamiento de datos personales únicamente cuando dicho tratamiento se encuentre justificado por finalidades concretas, lícitas, explícitas y legítimas, en relación con las atribuciones que la normatividad aplicable le confiera.
- **Lealtad.** El responsable no deberá obtener datos personales a través de medios engañosos o fraudulentos.

- **Proporcionalidad.** Exige que cualquier tratamiento no vaya más allá de lo necesario para alcanzar sus objetivos. Así, se establece el deber de tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
- **Información.** Consiste en el deber de comunicar al titular de los datos información suficiente acerca de la existencia y características principales del tratamiento al que serán sometidos los datos personales, a través del aviso de privacidad.
- **Responsabilidad.** Impone al responsable la obligación de implementar mecanismos necesarios para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en esta ley, así como el deber de rendir cuentas al titular con relación al tratamiento de los datos personales que estén en su posesión.

Este Título tiene un impacto notable al adoptar el principio internacionalmente conocido como *accountability*. El reconocimiento de este principio no es nuevo, y figura en el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico. El principio de responsabilidad incluido en este documento es el siguiente: “Todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios señalados [anteriormente]”.

El Capítulo II de este Título consagra el deber de seguridad y las acciones para el establecimiento y mantenimiento de medidas de seguridad; los elementos que deberá contener el documento de seguridad; los factores para determinar la implementación de medidas de seguridad; los supuestos para actualizar el documento de seguridad, así como la implementación de medidas correctivas para adecuar las medidas de seguridad. Además, se delinea en términos generales el deber de confidencialidad.

En este sentido, se establece que las medidas de seguridad para el tratamiento de datos personales deben estar documentadas y contenidas en un sistema de gestión, entendido como un 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 ley y las demás disposiciones que le resulten aplicables en la materia.

El Título III está dedicado a la regulación de los derechos de acceso, rectificación, cancelación y oposición, comúnmente reconocidos por su acrónimo como derechos ARCO. En el Capítulo I de este Título se establecen los alcances y contenido de cada uno de los derechos. En el Capítulo II se establecen los requisitos para acreditar la identidad del titular en el ejercicio de los derechos ARCO; la previsión sobre la gratuidad en su ejercicio; los plazos para su ejercicio; los requisitos que debe contener la solicitud para su ejercicio; las excepciones al ejercicio de estos derechos y la posibilidad de interponer el recurso de revisión en caso de que se actualice la negativa para dar trámite a la solicitud de derechos ARCO, o bien, por falta de respuesta de los responsables del tratamiento.

El derecho de acceso ha sido incluido en la ley señalando que el titular o su representante podrán conocer sus datos personales que obren en posesión de los responsables, así como la información relacionada con las condiciones y generalidades de su tratamiento. Mediante el reconocimiento del derecho de acceso, se confiere a los titulares tanto la

prerrogativa de acceder a sus datos personales como el derecho a conocer las condiciones a las que están sometidos los mismos.

Ahora bien, el derecho de rectificación concede al titular de los datos la posibilidad de solicitar a los responsables la corrección de su información personal, cuando esta sea inexacta, incompleta o no se encuentre actualizada.

En este Título se han incluido por primera vez en un ordenamiento de protección de datos del sector público federal los derechos de cancelación de datos personales y de oposición al tratamiento de los mismos. Con el reconocimiento de los derechos de cancelación y oposición, los titulares tienen la facultad de solicitar respectivamente, la supresión o eliminación de sus datos personales que se encuentren en bases de datos o archivos de responsable, o bien, solicitar la oposición al tratamiento de los datos en supuestos específicos.

Al respecto, cabe destacar que debido a que como regla general los entes y organismos del sector público llevan a cabo el tratamiento de datos personales habilitados por una norma o disposición jurídica, el derecho de los titulares a suprimir su información y a oponerse a su tratamiento, se circunscribe a aquellos casos que actualicen las hipótesis siguientes:

- Exista una causa legítima para llevar a cabo el tratamiento y su situación concreta así lo requiera, lo cual implica que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que se ocasione un daño o perjuicio al titular.
- El titular no desee que se lleve a cabo el tratamiento de sus datos personales para fines específicos, siempre y cuando dicho tratamiento no sea necesario para el cumplimiento de una obligación legal por parte del titular o el responsable.
- Los 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, localización, estado de salud, preferencias personales, fiabilidad o comportamiento.

Entre los efectos altamente positivos de regular el derecho de cancelación está la posibilidad de que los particulares cuenten con un mecanismo para hacer efectivo su derecho al olvido ante cualquier responsable y particularmente empresas que actúan en determinadas plataformas y herramientas informáticas en Internet.

En este sentido, el presente documento de trabajo coincide en la necesidad de normar el derecho al olvido, en este caso por medio del derecho de cancelación, previsto en el anteproyecto COMAIP, y así dotar a los particulares de herramientas jurídicas útiles para hacer frente a los posibles efectos no deseados de los desarrollos tecnológicos.

Con este reconocimiento se confiere máxima fuerza al derecho de autodeterminación informativa de los titulares pues cuentan con mecanismos para mantener el control sobre su información personal en todo momento.

Al igual que en el anteproyecto COMAIP, en el presente documento de trabajo se reconocen los cuatro derechos fundamentales de que debe gozar todo titular de datos personales: acceso, rectificación, cancelación y oposición.

El Título IV se compone de un Capítulo Único y versa sobre la relación entre responsable y encargado. En este Capítulo se han incluido cuestiones tales como la naturaleza y alcance de la figura del encargado; la formalización de la relación jurídica entre responsable y encargado; las consecuencias del incumplimiento de las obligaciones del encargado; la subcontratación de servicios; la formalización de la relación jurídica entre encargado y subcontratado; y la contratación de servicios de cómputo en la nube.

El documento de trabajo se crea en un contexto en el que existe una necesidad e interés creciente de que los responsables del tratamiento garanticen la adopción de medidas eficaces para una auténtica protección de datos.

Por otra parte, este Título establece un régimen para regular las relaciones jurídicas entre los responsables y encargados. Se ha referido anteriormente que un elemento característico de la figura del encargado es que lleva a cabo el tratamiento de datos personales por cuenta del responsable. Así, en la medida que se actualiza una especie de delegación de funciones en el tratamiento de datos personales, pero siempre aplicando las instrucciones dadas por el responsable cuando menos en lo relativo a los fines del tratamiento, el documento de trabajo establece que dicha relación debe formalizarse mediante un contrato o cualquier otro instrumento que decida el responsable. La utilidad de suscribir un contrato es, por una parte, acreditar la existencia, alcance y contenido de la relación jurídica; por otro lado, tiene como propósito asegurar el cumplimiento de las obligaciones del encargado conforme al mandato conferido por el responsable.

Adicionalmente, conscientes de la necesidad de adaptar las cláusulas contractuales a la dimensión transnacional del tratamiento de datos personales, y teniendo en cuenta la extendida práctica de la "subcontratación de servicios", se ha incluido un artículo que habilita al encargado para, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales siempre y cuando medie la autorización expresa del responsable. En tal supuesto, el subcontratado asumirá el carácter de encargado en términos de este ordenamiento y demás disposiciones que resulten aplicables en la materia.

En esta misma línea, es destacable que el documento de trabajo establezca un parámetro para adjudicar responsabilidad al encargado cuando este incumpla las instrucciones dadas por el responsable y decida por sí mismo sobre el tratamiento de los datos personales. En tal supuesto, el encargado asumirá el carácter de responsable conforme a la legislación que resulte aplicable. Esto en línea con los estándares internacionales.

En un mundo tecnológicamente globalizado, en donde la prestación de servicios y el tratamiento sistemático de información se realizan a través de Internet y a través medios electrónicos y digitales, se ha incluido un artículo que refiere a la contratación de servicios de cómputo en la nube. En este supuesto, sobresale la previsión para el responsable consistente en que podrá contratar los servicios de un proveedor de servicios, aplicaciones e infraestructura en el denominado cómputo en la nube y otras materias, siempre y cuando garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en el documento de trabajo.

El Título V está compuesto por un solo Capítulo, destinado a establecer las reglas básicas para la realización de transferencias y remisiones de datos personales. Al respecto, cabe tener presente que conforme al apartado de definiciones, el término genérico es el de comunicación de datos personales, mismo que comprende cualquier transferencia o remisión de datos personales realizada por el responsable a una persona distinta del titular.

Al respecto, la transferencia implica toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado; y la remisión ha sido definida como toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

La regulación de las comunicaciones de datos es un tema central puesto que permite mantener un nivel estándar u homogéneo de protección aun cuando los datos se encuentren en constante flujo. Las transferencias, como una especie del tratamiento de datos, quedan sujetas originalmente al consentimiento del titular de los datos, salvo que se actualicen las excepciones siguientes:

- Cuando la transferencia esté prevista en una ley, convenio o tratado internacional suscrito y ratificado por México.
- 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.
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.
- 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.
- 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.
- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

Por primera vez en la legislación federal mexicana, en el ámbito público, se contaría con reglas que de manera clara establecen el mecanismo a través de cual se puede transferir información válidamente, dentro y fuera de territorio nacional, cuestión que para nada resulta menor, ya que se trata de uno de los pilares sobre los que se erige en el derecho comparado este derecho fundamental.

En el Título VI relativo a acciones preventivas refiere a dos temas novedosos que se han incluido en el documento de trabajo. Por una parte, el Capítulo I aborda cuestiones relativas a la evaluación de impacto a la protección de datos personales, y el Capítulo II versa sobre mejores prácticas que los responsables podrán desarrollar o adoptar para el cumplimiento de las obligaciones previstas.

La elaboración de una evaluación de impacto a la protección de datos personales constituye una enorme aportación en materia de privacidad y datos personales. Dicha evaluación permitirá identificar y mitigar los impactos y amenazas que puedan comprometer los principios y deberes que rigen el tratamiento de los datos personales, así como los derechos de los titulares. De la misma manera, busca prevenir riesgos que pudieran producirse en los titulares respecto al tratamiento de su información personal.

Conforme a lo establecido en el documento de trabajo, la evaluación de impacto a la protección de datos personales deberá presentarse cuando los responsables elaboren anteproyectos de leyes, decretos o actos administrativos de carácter general, o bien, pretendan poner en operación o modificar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales.

Por otra parte, se propone la adopción de esquemas mínimos de mejores prácticas con la finalidad de:

- Elevar el nivel de protección de los datos personales.
- Armonizar el tratamiento de datos personales en un sector específico.
- Facilitar el ejercicio de los derechos ARCO por parte de los titulares.
- Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales.
- 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.

Dichos esquemas deberán ser reconocidos por el Instituto y cumplir con los parámetros que éste o los organismos garantes emitan conforme a los criterios emitidos por el primero. Asimismo, deberán ser notificados al Instituto o a los organismos garantes según corresponda.

En el Título VII se regula el Registro Nacional de Protección de Datos Personales, aspecto en el que el presente documento de trabajo coincide con el anteproyecto COMAIP, en el sentido de contar con un mecanismo que dé cuenta de la existencia de sistemas de datos personales en posesión de los sujetos obligados.

Este Título conformado por un Capítulo Único, en él se sientan las bases para la creación de un Registro Nacional de Protección de Datos que tenga por objeto transparentar y hacer del conocimiento del público en general información sobre las bases de datos personales en posesión de cualquier ente público, independientemente del nivel de gobierno.

La inscripción de las bases de datos personales que traten los responsables será obligatoria y deberá señalarse respecto de estas cuando menos la siguiente información:

- El nombre de la base de datos personales;
- La normatividad aplicable que dé fundamento a la creación, modificación o supresión de la base de datos personales;

- La finalidad de la base de datos personales, y
- El tipo de datos personales objeto de tratamiento.

Para la operación, funcionamiento y administración del Registro, el Instituto definirá las reglas de operación, mismas que regirán el suministro, intercambio y sistematización de la información del Registro.

El Título VIII se compone de dos Capítulos. El Capítulo I está dedicado a referir la integración del Comité de Transparencia; señalar sus atribuciones y a establecer la creación de la figura del oficial de protección de datos personales. El Capítulo II prevé las atribuciones de la Unidad de Transparencia, así como el procedimiento para la designación del titular de la misma.

En este Título, y continuando con el modelo actual en materia de acceso a la información, el Comité de Transparencia se erige como la autoridad máxima en materia de protección de datos personales y sus resoluciones serán adoptadas por mayoría de votos.

Por otra parte, se crea la figura del oficial de protección de datos personales como parte del Comité de Transparencia y con el carácter de especialista en la materia. Esto resulta muy relevante en la óptica de dar la relevancia que merece el tema. De manera que las decisiones que se adopten sean siempre desde el conocimiento y pericia que este especialista pueda aportar más allá de la preparación que los otros miembros del Comité hagan de cada una de las sesiones. De este modo se garantiza un grado mínimo de especialización, en una materia de índole técnico, en el seno de la instancia máxima en materia de datos en cada sujeto regulado.

Respecto a las atribuciones de la Unidad de Transparencia, y con la finalidad de garantizar el ejercicio del derecho a la protección de datos personales, se prevé que los responsables deberán promover acuerdos con instituciones públicas para atender las solicitudes presentadas en lenguas indígenas.

El Título IX se integra por tres Capítulos. En su Capítulo I destacan las atribuciones del Instituto en materia de protección de datos personales. El Capítulo II señala las atribuciones de los organismos garantes para los efectos de este ordenamiento y el Capítulo III tiene como objeto establecer las bases de la coordinación y promoción del derecho a la protección de datos personales.

Entre las atribuciones del Instituto se destaca la relativa a conocer, sustanciar 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 este punto también destaca la coincidencia ente el anteproyecto COMAIP y el presente documento de trabajo en el sentido de que en el diseño de ambos se advirtió la necesidad de contar con un esquema de distribución de competencias entre el organismo garante nacional y los organismos garantes estatales y del Distrito Federal.

En materia de medios de impugnación en el Título X se establecen tres mecanismos que son el recurso de revisión, el recurso de inconformidad y la facultad de atracción.

Complementariamente se establece un Capítulo sobre criterios de interpretación que establece los tipos de criterio que se pueden generar y su forma de sistematizar y compilar, entre otras reglas.

El recurso de revisión se establece como el medio de defensa que los particulares tienen frente a un presunto actuar indebido por parte de los sujetos obligados en materia de solicitudes de derechos ARCO. Este medio de defensa está diseñado para promoverse ante el organismo garante a nivel nacional o ante los organismos garantes estatales.

El recurso de inconformidad constituye un elemento novedoso de la reforma constitucional de febrero de este año, ya que establece la posibilidad de que los particulares para impugnar la resolución del recurso de revisión emitido por un organismo garante estatal frente al organismo garante a nivel nacional. De este modo se reconoce una nueva instancia a los particulares para hacer efectivos sus derechos frente a una instancia especializada sin necesidad de acudir a los tribunales.

Cabe destacar que tanto para el ejercicio de derechos ARCO como para la presentación de los medios de defensa descritos (recurso de revisión e inconformidad) se habilita expresamente la posibilidad de que se actúe en relación con datos personales que correspondieron a personas fallecidas, cuestión sin precedentes en la legislación federal mexicana en la materia.

Con los medios de impugnación se busca proveer de los mecanismos de tutela que como mínimo se deben garantizar en todos los niveles de gobierno para hacer efectivo este derecho ante presuntas actuaciones indebidas por parte de los sujetos obligados.

Destaca que para efectos de la facultad de atracción especialmente se tomaron en cuenta los parámetros que ha dictado el Máximo Tribunal en materia de interés y trascendencia, a efecto de que los casos que por esta ruta se conozcan resulten relevantes, novedosos, de notable importancia, complejos o que tengan un impacto o repercutan en los valores sociales, políticos o de convivencia, bienestar o estabilidad del Estado mexicano.

Por lo que refiere al recurso de inconformidad, se buscó desarrollar una herramienta eficiente y poderosa para el ciudadano pero a la vez respetuosa de los espacios de los organismos garantes estatales y del Distrito Federal.

Este Título XI, conformado por un Capítulo Único, aborda cuestiones relativas a la facultad de vigilancia y verificación que tienen el Instituto y los organismos garantes, en el ámbito de sus respectivas competencias, del cumplimiento de las disposiciones contenidas en la Ley y demás ordenamientos que de ella se deriven.

Se establecen las causales del procedimiento de verificación, señalando que ésta podrá iniciarse de oficio cuando el Instituto o los organismos garantes cuenten con indicios que hagan presumir fundada y motivadamente la existencia de violaciones a las leyes correspondientes, o bien, por denuncia de cualquier persona.

Aclarando que el procedimiento de verificación no procederá en los supuestos establecidos expresamente como causales de procedencia de recurso de revisión, se reconocen las

facultades del Instituto o los organismos garantes, de desarrollar investigaciones previas, con el fin de contar con elementos suficientes para fundar y motivar la orden de verificación respectiva.

En este Título también se incluyen los requisitos para presentar una denuncia, entre los que se encuentran los siguientes:

- El nombre del denunciante o de su representante, en su caso.
- El domicilio del denunciante o cualquier otro medio para recibir notificaciones.
- La relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho.
- La denominación y domicilio del responsable denunciado o, en su caso, los datos para su identificación y/o ubicación.
- La firma del titular afectado o denunciante, o en su caso, de su representante. En caso de no saber firmar, bastará la huella digital.

Respecto del procedimiento de inicio de una verificación, se establece que esta iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los organismos garantes. El procedimiento de verificación deberá tener una duración máxima de ciento ochenta días, el cual podrá ampliarse por un periodo igual por una sola vez.

El Título XII se compone de dos Capítulos. El Capítulo I está destinado a establecer las medidas de apremio para asegurar el cumplimiento de las resoluciones del Instituto y los organismos garantes. Las medidas de apremio adoptadas en esta Ley son las siguientes:

- La amonestación.
- La multa, de ciento cincuenta hasta mil quinientas veces el salario mínimo general vigente en el área geográfica de que se trate.

Las medidas de apremio a que se refiere el presente Capítulo serán 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.

El Capítulo II incluye uno de los temas más importantes en relación con la aplicación eficiente de un orden jurídico, es el caso específico de los supuestos de responsabilidad administrativa de los servidores públicos y el régimen de sanciones. El régimen de responsabilidades está relacionado precisamente con el incumplimiento de las obligaciones de los servidores públicos legalmente establecidas. Este incumplimiento es el detonante de la instauración de un procedimiento de responsabilidad administrativa y en su caso, de la consecuente aplicación de la sanción correspondiente.

En virtud de lo antes expuesto se somete a la consideración de esta H. Cámara de Senadores:

DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS.

ARTÍCULO ÚNICO.- Se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Título I Disposiciones Generales

Capítulo I Del objeto de la ley

Objeto

Artículo 1. La presente ley es de orden público y de observancia general en toda la República, es reglamentaria de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

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 o tratamiento de los sujetos obligados.

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

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 se regirán por la ley federal de la materia.

Objetivos específicos

Artículo 2. Son objetivos de la presente ley:

- I. Distribuir competencias entre la Federación, los Estados, el Distrito Federal, los municipios y las delegaciones del Distrito Federal, en materia de protección de datos personales en posesión de sujetos obligados;
- II. Establecer las bases mínimas que regirán los procedimientos para garantizar el ejercicio del derecho de protección de datos personales en posesión de sujetos obligados;
- III. Establecer los procedimientos y condiciones homogéneas que regirán el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales, mediante procedimientos sencillos y expeditos;
- IV. Regular la de 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 en materia de transparencia, en lo relativo a sus funciones para la protección de datos personales

- V. 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;
- VI. 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 en los ámbitos federal, estatal o municipal, con la finalidad de regular su debido tratamiento.
- VII. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;
- VIII. Promover, fomentar y difundir una cultura de protección de datos personales;
- IX. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio y las sanciones que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta ley.

Definiciones

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

- I. Área:** Instancias de los sujetos obligados previstas en el reglamento interior, estatuto orgánico respectivo o equivalentes que cuentan, dan tratamiento, son responsables o encargados de los datos personales;
- II. Aviso de privacidad:** Documento físico, electrónico o en cualquier formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle las características principales del tratamiento al que serán sometidos sus datos personales;
- III. Bases de Datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado 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 supresión en la base de datos que corresponde;
- V. 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;
- VI. 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;
- VII. Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular que autoriza el tratamiento de sus datos personales;
- VIII. 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, siempre y cuando esto no requiera plazos o actividades desproporcionados;

- IX. Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;
- X. Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;
- XI. Días:** Días hábiles;
- XII. 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;
- XIII. Encargado:** Persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable;
- XIV. Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultados por cualquier persona no impedida 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;
- XV. Instituto:** Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales;
- XVI. Evaluación de impacto a la protección de datos personales:** Documento mediante el cual se da a conocer la evaluación que permite determinar los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar riesgos que puedan comprometer los principios, deberes y derechos de los titulares previstos en la normativa aplicable;
- XVII. 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;
- XVIII. Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;
- XIX. 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., 116, fracción VIII y 122, apartado C, BASE PRIMERA, Fracción V, inciso ñ) de la Constitución Política de los Estados Unidos Mexicanos;
- XX. 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;
- XXI. Registro:** Registro Nacional de Protección de Datos Personales;
- XXII. Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

- XXIII. Responsable:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, así como los fideicomisos y fondos públicos que traten datos personales;
- XXIV. Sistema Nacional:** Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;
- XXV. Supresión:** Actividad consistente en eliminar, borrar o destruir los datos personales bajo las medidas de seguridad previamente establecidas por el responsable. Para efectos de la presente ley, por eliminar, borrar o destruir, se entenderá la baja archivística de los datos personales conforme a la normativa archivística que resulte aplicable;
- XXVI. Titular:** Persona física a quien pertenecen los datos personales;
- XXVII. Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;
- XXVIII. Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas con la obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación o disposición de datos personales, y
- XXIX. Unidad de Transparencia:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

Excepciones generales del derecho a la protección de datos personales

Artículo 4. Los principios, deberes y derechos previstos en la presente ley tendrán como límite en cuanto a su observancia y ejercicio la protección de la seguridad nacional, las disposiciones de orden público, la seguridad y salud públicas, o los derechos de terceros.

Tratamiento de datos personales de carácter sensible

Artículo 5. Por regla general no podrán tratarse datos personales sensibles, salvo que los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones previstas en las normas que regulan la actuación del responsable.

Tratamiento de datos personales de menores de edad

Artículo 6. En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior del niño, la niña y el adolescente.

Libertad de expresión y prensa

Artículo 7. El cumplimiento de los principios, deberes y derechos previstos en la presente ley podrá exentarse únicamente en la medida en que resulte necesario conciliar el derecho a la protección de datos personales con el derecho a la libertad de expresión y prensa, conforme a las reglas que se establezcan en la ley federal y las de las entidades federativas.

Reglas de interpretación

Artículo 8. En la aplicación e interpretación de la presente ley se estará a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales de los que el Estado Mexicano sea parte, así como en las resoluciones, sentencias, determinaciones, decisiones, criterios y opiniones vinculantes, entre otros, que emitan los órganos internacionales especializados, privilegiando en todo momento la interpretación que más favorezca a los solicitantes.

Capítulo II

Del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Alcance y objeto del Sistema Nacional

Artículo 9. El Sistema Nacional se conformará de acuerdo con la Ley General de Transparencia y Acceso a la Información Pública. En materia de protección de datos personales, tiene como función coordinar y evaluar las acciones relativas a la política pública transversal de protección de dicho derecho, así como establecer e implementar los criterios y lineamientos, de conformidad con lo señalado en la presente ley, la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable

Artículo 10. 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. Este esfuerzo conjunto e integral, contribuirá 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 de Protección de Datos Personales

Artículo 11. Además de los objetivos previstos en la Ley General de Transparencia y Acceso a la Información Pública Gubernamental, 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:

- I. Promover la educación y una cultura de protección de datos personales entre la sociedad mexicana;
- II. Fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición;
- III. Capacitar a los servidores públicos en materia de protección de datos personales;
- IV. Emitir lineamientos generales para el debido tratamiento de los datos personales;
- V. Emitir lineamientos para homologar el ejercicio de los derechos ARCO;
- VI. Impulsar la implementación y mantenimiento de un sistema de gestión de seguridad a que se refiere el artículo 31 de la presente ley, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia, y
- VII. Prever los mecanismos que permitan medir, reportar y verificar las metas establecidas.

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.

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

Consejo Nacional

Artículo 12. El Sistema Nacional contará con un Consejo Nacional. En la integración, organización, funcionamiento y atribuciones del Consejo Nacional se estará a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables.

Funciones del Sistema Nacional

Artículo 13. 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 en toda la República Mexicana;
- II. Fomentar entre la sociedad una cultura de protección de los datos personales;
- III. Analizar, opinar y proponer a las instancias facultadas para ello proyectos de reforma o modificación de la normativa en la materia;
- IV. Acordar y establecer los mecanismos de coordinación que permitan la formulación y ejecución de instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendientes 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 para el funcionamiento del Sistema Nacional;
- VI. Formular, establecer y ejecutar políticas generales en materia de protección de datos personales;
- VII. 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. Promover la homologación y desarrollo de los procedimientos previstos en la presente ley y evaluar sus avances;
- IX. Diseñar e implementar políticas en materia de protección de datos personales;
- X. 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 comunes de alcance nacional para medir el cumplimiento y los avances de los responsables;
- XII. Suscribir convenios de colaboración que tengan por objeto coadyuvar al cumplimiento de los objetivos del Sistema Nacional y aquéllos previstos en la presente ley y demás disposiciones que resulten aplicables en la materia;

- XIII. 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 o modelos en materia de protección de datos personales;
- XV. Promover la comunicación y coordinación con autoridades nacionales, federales, de los Estados y el Distrito Federal, municipales y autoridades y organismos internacionales, con la finalidad de impulsar y fomentar los objetivos de la presente ley;
- XVI. Proponer acciones para vincular el Sistema Nacional con otros sistemas y programas nacionales, regionales o locales;
- XVII. 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 en materia de transparencia y acceso a la información pública y demás normativa aplicable, y
- XVIII. Las demás que se establezcan en otras disposiciones en la materia para el funcionamiento del Sistema Nacional.

Organización y funcionamiento del Consejo Nacional

Artículo 14. El Consejo Nacional funcionará conforme a lo dispuesto en la ley general en materia de transparencia y acceso a la información pública y demás ordenamientos aplicables.

Título II Principios y Deberes

Capítulo I De los Principios

Principios generales de protección de datos personales

Artículo 15. El responsable deberá observar los principios de licitud, lealtad, consentimiento, calidad, finalidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales.

Principio de licitud

Artículo 16. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera.

El responsable deberá realizar el tratamiento de datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por la legislación mexicana y el derecho internacional que resulte aplicable.

Principio de lealtad

Artículo 17. El responsable no deberá obtener datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Principio del consentimiento

Artículo 18. Todo tratamiento de datos personales en posesión del responsable deberá contar con el consentimiento previo del titular, salvo en los casos previstos en el artículo 20 de la presente ley, el cual deberá otorgarse de forma:

- 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.

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

Modalidades del consentimiento

Artículo 19. 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. El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, salvo que la ley exija que la voluntad del titular se manifieste expresamente.

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 siguiente artículo.

Excepciones al principio del consentimiento

Artículo 20. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

- I.** Cuando una ley así lo disponga;
- II.** Para las transferencias que se realicen entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas a la finalidad que motivó el tratamiento de los datos personales;
- III.** Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- IV.** Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- V.** Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- VI.** Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

- VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria; tratamientos médicos, o la gestión de servicios sanitarios, o
- VIII. Cuando los datos personales figuren en fuentes de acceso público. Este supuesto será aplicable únicamente en el caso de que los datos personales que obren en la fuente de acceso público tengan una procedencia lícita conforme a las disposiciones establecidas en la presente ley y demás normativa aplicable.

Principio de calidad

Artículo 21. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

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.

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.

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 a la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Principio de finalidad

Artículo 22. 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.

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 ley y medie el consentimiento del titular, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

Principio de proporcionalidad

Artículo 23. El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Principio de información

Artículo 24. 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.

Por regla general, el aviso de privacidad deberá ser puesto a disposición del titular de manera previa a la obtención de los datos personales.

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.

Aviso de privacidad

Artículo 25. El aviso de privacidad que el responsable ponga a disposición del titular previo al tratamiento de sus datos personales deberá contener la siguiente información:

- I.** El responsable;
- II.** Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
- III.** Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
 - a)** Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y
 - b)** Las finalidades de estas transferencias;
- IV.** Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular;
- V.** El sitio donde se podrá consultar el aviso de privacidad con la información que establece el artículo siguiente;
- VI.** 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 refiere el artículo siguiente.

Aviso de privacidad

Artículo 26. El aviso de privacidad al que refiere la fracción V del artículo anterior deberá contener, al menos, la siguiente información:

- I.** El responsable y su domicilio;
- II.** Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
- III.** El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
- IV.** Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;
- V.** Las transferencias de datos personales que en su caso se efectúen, requieran o no el consentimiento del titular;

- a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales;
 - b) Las finalidades de las transferencias de datos personales, distinguiendo las transferencias que requieren el consentimiento del titular, y
 - c) El fundamento que faculte al responsable para llevarlas a cabo;
- VI. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
 - VII. El domicilio de la Unidad de Información;
 - VIII. 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 que requieren del consentimiento del titular, y
 - IX. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Los mecanismos y medios a los que refieren la fracción VIII del presente artículo y la fracción IV del artículo anterior, 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.

Instrumentación de medidas compensatorias

Artículo 27. Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o personal, 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 Instituto y los organismos garantes, conforme a los criterios que fije el primero.

Se entiende que el aviso de privacidad se da a conocer de manera directa cuando se hace del conocimiento del titular por algún medio que permite su entrega directa, como se señala de manera enunciativa mas no limitativa el correo postal, medio electrónico o vía telefónica, entre otros.

Se entiende que el aviso de privacidad se da a conocer personalmente cuando el responsable o la persona designada para tal fin entrega o hace del conocimiento del titular el aviso de privacidad, con la presencia física de ambos.

Principio de responsabilidad

Artículo 28. El responsable deberá implementar los mecanismos necesarios para acreditar el cumplimiento de los principios, deberes y obligaciones establecidas en la presente ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto o los organismos garantes, según corresponda, para lo cual podrá

valerse de estándares, mejores prácticas nacionales o internacionales o de cualquier otro mecanismo que determine adecuado para tales fines.

Lo anterior aplicará aun y cuando los datos personales sean tratados por parte de un encargado a solicitud del responsable, así como al momento de realizar transferencias de datos personales.

Mecanismos para cumplir con el principio de responsabilidad

Artículo 29. 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 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 del responsable;
- III.** 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 de seguridad de datos personales para determinar las modificaciones que se requieran;
- V.** 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
- VI.** 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.

Remisión a leyes secundarias

Artículo 30. La ley federal y las leyes de las entidades federativas que en la materia resulten aplicables para el cumplimiento de la presente ley, deberán desarrollar las obligaciones específicas que den contenido a los principios de protección de datos personales previstos en el presente ordenamiento.

Capítulo II De los Deberes

Deber de seguridad

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.

Artículo 32. 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.** La pérdida o destrucción no autorizada;
- II.** El robo, extravío o copia no autorizada;
- III.** El uso, acceso o tratamiento no autorizado, o
- IV.** El daño, la alteración o modificación no autorizada.

Bitácora

Artículo 33. Los responsables deberán 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.

Notificación de vulneraciones de seguridad

Artículo 34. El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

Información mínima al titular en caso de vulneraciones de seguridad

Artículo 35. El responsable deberá informar al titular al menos lo siguiente:

- I.** La naturaleza del incidente;
- II.** Los datos personales comprometidos;
- III.** Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- IV.** Las acciones correctivas realizadas de forma inmediata, y
- V.** Los medios donde puede obtener más información al respecto.

Medidas de seguridad

Artículo 36. Las medidas de seguridad pueden ser:

1. 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;

2. 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 mas no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que puedan salir de la organización, y Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad e integridad;

3. 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:

- a) 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 el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- c) 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 en el tratamiento de datos personales;

Factores para determinar la implementación de medidas de seguridad

Artículo 37. Las medidas de seguridad adoptadas por el responsable deberán considerar:

- I. El riesgo inherente a los datos personales tratados;
- II. La sensibilidad de los datos personales tratados;
- III. El desarrollo tecnológico;
- IV. Las posibles consecuencias de una vulneración para los titulares;
- V. Las transferencias de datos personales que se realicen;
- VI. El número de titulares;
- VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
- VIII. 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.

Acciones para el establecimiento y mantenimiento de medidas de seguridad

Artículo 38. 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, 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 en el tratamiento de datos personales;
- III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- IV. 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, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
- VI. 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 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 bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Sistema de gestión y documento de seguridad

Artículo 39. 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.

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.

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

- I. El inventario de datos personales y de los sistemas de tratamiento;
- II. Las funciones y obligaciones de las personas que traten datos personales;
- III. El análisis de riesgos;

- IV. El análisis de brecha;
- V. El plan de trabajo;
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- VII. El programa general de capacitación.

Actualización del documento de seguridad

Artículo 40. El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

- I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- II. Como resultado de un proceso de mejora continua derivado del monitoreo y revisión del sistema de gestión, y
- III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.

Implementación de acciones correctivas y preventivas ante una vulneración de seguridad

Artículo 41. 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.

Deber 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 sigilo respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el mismo.

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

Título III

Derechos de los Titulares y su Ejercicio

Capítulo I

De los Derechos de Acceso, Rectificación, Cancelación y Oposición

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. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

Derecho de acceso

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 de rectificación

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

Derecho de cancelación

Artículo 46. El titular tendrá derecho a solicitar la supresión 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

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

- I.** Exista una causa legítima y su situación específica así lo requiera, lo cual implica que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, o
- II.** No desee que se lleve a cabo el tratamiento de sus datos personales para fines específicos.
- III.** 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, localización, estado de salud, preferencias personales, fiabilidad o comportamiento.

Capítulo II

Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición

Gestión de solicitudes 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 Capítulo y demás disposiciones que resulten aplicables en la materia.

Acreditación de la identidad del titular

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.

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

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.

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico o legítimo podrá ejercer los derechos que confiere el presente Capítulo, conforme a la normativa aplicable.

Gratuidad en el ejercicio de los derechos ARCO

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.

Las cuotas de los derechos aplicables deberán establecerse en la Ley Federal de Derechos, los cuales se publicarán en los sitios de Internet de los responsables. En su determinación se deberá considerar que los montos permitan o faciliten el ejercicio de los derechos ARCO.

Los responsables a quienes no les sea aplicable la Ley Federal de Derechos deberán establecer cuotas que no deberán ser mayores a las dispuestas en dicha ley.

Cuando la reproducción implique la entrega de no más de veinte hojas simples, éstas deberán ser entregadas sin costo alguno. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular del derecho.

Para el caso de los costos de envío, dicho fin se procurará a través de la celebración de convenios que reduzcan sus montos.

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.

Plazo para el ejercicio de los 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.

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.

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 de la solicitud para el ejercicio de los derechos ARCO

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

- I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
- II. Los documentos que acrediten la identidad del titular, y en su caso, la personalidad e identidad de su representante;
- III. El área responsable que trata los datos personales y ante el cual se presenta la solicitud;
- IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO;
- V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y
- VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. En el caso de una solicitud de rectificación, se deberán señalar las modificaciones a realizarse y aportar la documentación que dé sustento a la petición.

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. En 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.

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable que el titular considere competente, a través de escrito

libre, o formatos, medios electrónicos o cualquier otro medio que al efecto establezca el responsable.

Trámites específicos

Artículo 53. 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 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 del ejercicio de los derechos ARCO

Artículo 54. Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:

- I. Cuando el titular o su representante no estén debidamente acreditados para ello;
- II. Cuando los datos personales no se encuentren en posesión del responsable;
- III. Cuando exista un impedimento legal;
- IV. Cuando se obstaculicen actuaciones judiciales o administrativas;
- V. 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;
- VI. Cuando la cancelación u oposición haya sido previamente realizada respecto al mismo titular, responsable y datos personales;
- VII. Cuando el responsable no sea competente;
- VIII. Cuando se protejan intereses jurídicamente tutelados del titular, o
- IX. Cuando se dé cumplimiento a obligaciones legalmente adquiridas por el titular.

En los casos anteriores, el Comité de Transparencia deberá confirmar la negativa, fundando y motivando la misma; así como informar al titular del derecho 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, a través del medio señalado para oír notificaciones, acompañando, en su caso, las pruebas que resulten pertinentes.

Negativa al ejercicio de derechos ARCO

Artículo 55. 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.

Remisión a leyes secundarias

Artículo 56. La ley federal y las leyes de los Estados y del Distrito Federal que en la materia resulten aplicables para el cumplimiento de la presente ley, deberán desarrollar la forma, términos, plazos y procedimientos que regirán el ejercicio de los derechos ARCO de conformidad con las disposiciones previstas en el presente Capítulo.

Título IV Relación del Responsable y Encargado

Capítulo Único De las Figuras del Responsable y Encargado

Obligación general del encargado

Artículo 57. 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 jurídica entre responsable y encargado

Artículo 58. 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.

En el contrato o instrumento jurídico que decida el responsable se deberá 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 las instrucciones del responsable;
- II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
- V. Guardar confidencialidad respecto de los datos personales tratados;
- VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
- VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Los acuerdos entre 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.

Consecuencia del incumplimiento de las obligaciones del encargado

Artículo 59. 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 de servicios

Artículo 60. 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.

Formalización de la relación jurídica entre responsable y subcontratante

Artículo 61. 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.

Contratación de servicios de cómputo en la nube y otras materias

Artículo 62. El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el denominado 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.

Título V

Comunicaciones de Datos Personales

Capítulo Único

De las Transferencias y Remisiones de Datos Personales

Reglas generales para la realización de transferencias

Artículo 63. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en el artículo 67 y deberá ser informada al titular en el aviso de privacidad y limitarse a las finalidades que la justifiquen.

Formalización de transferencias de datos personales y excepciones

Artículo 64. En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se obligó a tratar los datos personales frente al titular.

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.

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

- I. 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. 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 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.

Transferencias nacionales de datos personales

Artículo 65. Cuando la transferencia sea nacional, el receptor de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable y deberá tratar los datos personales atendiendo a dicha legislación y a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

Transferencias internacionales de datos personales

Artículo 66. El responsable sólo podrá transferir datos personales fuera del territorio nacional cuando el tercero receptor 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.

Excepciones para realizar transferencias de datos personales sin consentimiento del titular

Artículo 67. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular en los siguientes supuestos:

- I. Cuando la transferencia esté prevista en una ley, convenio o tratado internacional suscrito y ratificado por México;
- II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular, o
- VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

Remisiones de datos personales

Artículo 68. 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 VI

Acciones Preventivas en Materia de Protección de Datos Personales

Capítulo I

De la Evaluación de Protección Datos Personales

Objeto de la Evaluación de Protección Datos Personales

Artículo 69. Cuando el responsable elabore anteproyectos de leyes, decretos o actos administrativos de carácter general relacionados con el tratamiento de datos personales, o bien, pretenda poner en operación o modificar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, los deberá presentar, según corresponda, ante el Instituto o los organismos garantes junto con una evaluación de impacto a la protección de datos personales.

El contenido de la evaluación de impacto a la protección de datos personales, así como los criterios para determinar que se está en presencia de un tratamiento intensivo o relevante de datos personales, deberán determinarse, según corresponda, por el Instituto y los organismos garantes conforme a los criterios que fije el primero.

Contenido mínimo de criterios

Artículo 70. Los criterios a que se refiere el artículo anterior deberán considerar, al menos, los siguientes rubros relacionados con el contenido de la evaluación de impacto a la protección de datos personales:

- I. El objeto, alcance, contenido, finalidades e información general y específica del anteproyecto normativo que se pretende elaborar, o bien, del programa, servicio, sistema de información o tecnología que se pretende implementar o modificar;
- II. El tipo de datos personales implicados y el público objetivo a quien impactaría directa o indirectamente el anteproyecto normativo, programa, servicio, sistema de información o tecnología;
- III. Las acciones concretas que permitan evaluar el nivel de cumplimiento de los principios, deberes y demás obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia, así como garantizar los derechos ARCO;
- IV. La identificación exhaustiva de los riesgos o amenazas potenciales que podrían menoscabar el derecho a la protección de datos personales de los titulares involucrados;
- V. Las acciones y controles específicos que permitan mitigar los riesgos potenciales que, en su caso, se detecten;
- VI.** La justificación que permita evidenciar la necesidad de emitir el anteproyecto normativo, o bien, implementar o modificar el programa, servicio, sistema de información o tecnología, y
- VII. Cualquier otra información adicional que el responsable considere importante hacer del conocimiento del Instituto o de los organismos garantes, para emitir el dictamen correspondiente.

El Instituto deberá definir en los criterios aludidos, los parámetros objetivos que permitan identificar al responsable cuando está en presencia de un tratamiento intensivo o relevante de datos personales, el cual amerite una evaluación de impacto a la protección de datos personales, en función de los siguientes factores:

- I.** El número de titulares;
- II. El público objetivo;
- III. Los riesgos inherentes a los datos personales a tratar;
- IV. La sensibilidad de los datos personales;
- V. Las transferencias de datos personales que se pretenden efectuar y su periodicidad, en su caso;

- VI. El desarrollo de la tecnología utilizada, en su caso;
- VII. La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue, y
- VIII. Los demás factores que el Instituto determine.

Plazo para la presentación de la evaluación de impacto a la protección de datos personales

Artículo 71. La presentación de la evaluación de impacto a la protección de datos personales a que se refiere el presente Capítulo, deberá hacerse, cuando menos, sesenta días anteriores a la fecha en que se pretenda emitir o someter a consideración de la instancia que corresponda el anteproyecto normativo, o en su caso, implementar o modificar la política pública, el programa, servicio, sistema de información o tecnología, a efecto de que el Instituto o los organismos garantes emitan el dictamen correspondiente.

Dictamen sobre la evaluación de impacto a la protección de datos personales

Artículo 72. El Instituto o los organismos garantes, según corresponda, deberán emitir un dictamen sobre la evaluación de impacto a la protección de datos personales del anteproyecto normativo, programa, servicio, sistema de información o tecnología presentado por el responsable, el cual deberá sugerir alternativas que permitan reducir la generación de los impactos y riesgos que se detecten en materia de protección de datos personales.

El plazo para la emisión del dictamen a que se refiere el párrafo anterior será dentro de los cuarenta días siguientes contados a partir del día siguiente a la presentación de la evaluación. Este plazo podrá ampliarse por veinte días más, siempre que existan causas justificadas para ello y la ampliación sea notificada al responsable interesado.

Sentido del dictamen

Artículo 73. El dictamen que emita el Instituto o los organismos garantes, según corresponda, podrá determinar la conformidad total o parcial o la no conformidad del anteproyecto normativo, programa, servicio, sistema de información o tecnología con las disposiciones que en materia de protección de datos personales resulten aplicables. En el dictamen de referencia el Instituto o los organismos garantes, según corresponda, emitirán las recomendaciones a que haya lugar.

Capítulo II De las Mejores Prácticas

Objeto de los esquemas de mejores prácticas

Artículo 74. 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 de los datos personales;
- II. Armonizar el tratamiento de datos personales en un sector específico;
- III. Facilitar el ejercicio de los derechos ARCO por parte de los titulares;
- IV. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y
- V. 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.

Validación o reconocimiento de los esquemas de mejores prácticas

Artículo 75. 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 para tal efecto emitan, según corresponda, el Instituto y los organismos garantes conforme a los criterios que fije el primero, y
- II. 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.

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.

Título VII Registro Nacional de Protección de Datos Personales

Capítulo Único Del Registro

Objeto del Registro

Artículo 76. El Registro es una aplicación informática administrada por el Sistema Nacional que tiene por objeto transparentar y hacer del conocimiento del público en general las bases de datos personales en posesión de cualquier responsable, así como facilitar a los titulares el ejercicio de los derechos ARCO.

La información de las bases de datos personales publicadas en el Registro es de carácter público y cualquier persona podrá consultarla de manera gratuita.

Obligación de inscripción en el Registro

Artículo 77. El responsable deberá inscribir en el Registro las bases de datos personales que trate, señalando respecto de las mismas, al menos, la siguiente información:

- I. El nombre de la base de datos personales;
- II. El responsable;
- III. La denominación de la unidad administrativa o área que administra la base de datos;
- IV. La normatividad aplicable que faculta al responsable a tratar los datos personales;
- V. La finalidad de la base de datos personales, y
- VI. El tipo de datos personales objeto de tratamiento.

La inscripción de una base de datos personales en el Registro, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la presente ley y demás disposiciones que resulten aplicables en la materia.

El responsable deberá actualizar el Registro cuando menos trimestralmente.

Aplicación informática gratuita

Artículo 78. El Sistema Nacional deberá poner a disposición una aplicación informática que permita la operación del Registro, de conformidad con el instrumento jurídico que al respecto establezca.

Emisión de reglas de operación del Registro

Artículo 79. El Sistema Nacional deberá emitir las reglas de operación que tengan por objeto definir el esquema a que se sujetarán los organismos garantes para el suministro, intercambio y sistematización de la información del Registro, y en general, su operación, funcionamiento y administración.

Título VIII

Comité de Transparencia y Unidad de Transparencia

Capítulo I

Comité de Transparencia

Integración del Comité de Transparencia

Artículo 80. 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.

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales, en la organización del responsable, el cual también estará integrado por el oficial de protección de datos personales cuando sesione para cuestiones relacionadas con esta materia.

Atribuciones del Comité de Transparencia

Artículo 81. 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. 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, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- III. 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 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, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- VI. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y
- VII. 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

Atribuciones de la Unidad de Transparencia

Artículo 82. Cada responsable contará con una Unidad 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.

Para los efectos de la presente ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, la Unidad de Transparencia, tendrá las siguientes funciones:

- I. 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;
- III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados o aquellos individuos que ejerzan derechos ARCO de personas fallecidas;
- IV. Informar al titular o su representante o a aquellos individuos que ejerzan derechos ARCO de personas fallecidas 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 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 instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
- VII. Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales.

En el caso de que se presenten solicitudes para el ejercicio de los derechos ARCO en lenguas indígenas, el responsable deberá promover acuerdos con la institución pública que pudiera auxiliarle con la finalidad de atender y dar respuesta a estas solicitudes en la lengua indígena correspondiente.

El responsable deberá implementar acciones para garantizar condiciones de accesibilidad para 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 83. 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.

Capítulo III Del Oficial de Protección de Datos Personales

Atribuciones del oficial de protección de datos personales

Artículo 84. El sujeto obligado responsable deberá designar a un oficial de protección de datos personales, el cual deberá fungir como enlace ante el Instituto o, en su caso, los organismos garantes para atender los asuntos relativos a la presente ley y demás normativa aplicable.

En la elección del oficial de protección de datos personales, el responsable deberá considerar que el candidato goce de experiencia en materia de protección de datos personales y que ocupe un cargo no menor a director general o su equivalente.

El oficial de protección de datos personales tendrá las siguientes atribuciones:

- I.** Asesorar al Comité de Transparencia respecto de los temas que sean sometidos a su consideración en materia de protección de datos personales;
- II.** Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente ley y demás disposiciones que resulten aplicables en la materia;
- III.** Inscribir en el Registro las bases de datos personales en posesión del responsable;
- IV.** Coordinar las acciones de capacitación en materia de protección de datos personales, e
- V.** Integrar y remitir el informe anual y demás informes requeridos por el Instituto o los organismos garantes, según corresponda, a efecto de verificar el cumplimiento de la presente ley y demás disposiciones que resulten aplicables en la materia.

Disposiciones específicas para partidos políticos

Artículo 85. Los partidos políticos deberán establecer en su regulación interna la integración, designación y atribuciones de los órganos a que se refiere el presente Título, en los términos previstos en la presente Ley y demás normativa que resulte aplicable en la materia.

Disposiciones específicas para los fideicomisos

Artículo 86. Los fideicomisos y fondos públicos que no cuenten con estructura orgánica y que no sean considerados entidades paraestatales deberán de dar cumplimiento a las obligaciones en materia de protección de datos personales, a través de la unidad administrativa responsable de coordinar su operación.

Título IX Organismos Garantes

Capítulo I

Del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Naturaleza jurídica del Instituto

Artículo 87. 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 y demás normativa aplicable.

En la elección de los comisionados del Instituto podrá tomarse en cuenta que el candidato goce de reconocida experiencia en materia de protección de datos personales, y de preferencia, que haya prestado servicios en dependencias, organismos o instituciones que ejerzan funciones de autoridad en materia de protección de datos personales.

Atribuciones del Instituto

Artículo 88. 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 Instituto tendrá las siguientes atribuciones:

- I. Garantizar el ejercicio del derecho a la protección de datos personales;
- II. Interpretar la presente ley en el ámbito administrativo;
- III. Conocer, sustanciar 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. Conocer, sustanciar 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, sustanciar 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 los procedimientos de verificación;
- VII. Imponer las medidas de apremio y sanciones previstas en términos de lo dispuesto por la presente ley y demás disposiciones que resulten aplicables en la materia, para asegurar el cumplimiento de sus resoluciones;
- VIII. 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 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, 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 para difundir y ampliar el conocimiento sobre la materia de la presente ley;
- XII. Proporcionar apoyo técnico a los responsables para el cumplimiento de las obligaciones establecidas en la presente ley;
- XIII. 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 contenidas en la presente ley;
- XV. Administrar el Registro y el registro de esquemas de mejores prácticas a que se refieren la presente Ley y emitir sus reglas de operación;

- XVI. Emitir los dictámenes correspondientes a las manifestaciones de impacto a la privacidad;
- XVII. 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;
- XVIII. 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;
- XIX. 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;
- XX. Presidir el Sistema Nacional a que se refiere el artículo 14 de la presente Ley;
- XXI. 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;
- XXII. Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales, así como de sus prerrogativas;
- XXIII. 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;
- XXIV. Promover la capacitación y actualización en materia de protección de datos personales entre los responsables;
- XXV. Emitir criterios generales de interpretación para garantizar el derecho a la protección de datos personales;
- XXVI. 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, y
- XXVII. 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 de Transparencia, a que se refiere la ley general en materia de transparencia y acceso a la información pública y demás normativa aplicable.

Capítulo II

De los Organismos Garantes

Naturaleza jurídica de los organismos garantes

Artículo 89. 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.

Atribuciones de los organismos garantes

Artículo 90. Para los efectos de la presente ley y sin perjuicio de otras atribuciones que les sean conferidas en la normatividad que le resulte aplicable, los organismos garantes tendrán las siguientes atribuciones:

- I. 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. Presentar a 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 las medidas de apremio y las sanciones previstas a que se refiere la presente ley y demás disposiciones que resulten aplicables en la materia, para asegurar el cumplimiento de sus resoluciones;
- IV. Promover y difundir el ejercicio del derecho a la protección de datos personales;
- V. 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, 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 para difundir y ampliar el conocimiento sobre la materia de la presente ley;
- VIII. 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 que le sean presentados, en términos de lo previsto en el Título X, Capítulo II de la presente ley y demás disposiciones que resulten aplicables en la materia;
- X. Suscribir convenios de colaboración con el Instituto para el cumplimiento de los objetivos previstos en la presente ley y demás disposiciones aplicables;
- XI. Vigilar, en el ámbito de sus respectivas competencias, el cumplimiento de la presente ley y demás disposiciones que resulten aplicables en la materia;
- XII. 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 respecto del cumplimiento de la presente ley y demás disposiciones que resulten aplicables;
- XIV. Promover la capacitación y actualización en materia de protección de datos personales entre los responsables;

- XV. Solicitar la cooperación del Instituto en los términos del artículo 88, fracción XXVI de la presente ley, y
- XVI. Administrar, en el ámbito de sus competencias, la Plataforma Nacional de Transparencia.

Capítulo III

De la coordinación y promoción del derecho a la protección de datos personales

Colaboración entre el Instituto y los organismos garantes

Artículo 91. 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.

Promoción del derecho a la protección de datos personales con instituciones educativas y organizaciones de la sociedad civil

Artículo 92. El Instituto y los organismos garantes, en el ámbito de sus respectivas competencias, deberán:

- I. 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 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 que estimulen el intercambio de ideas entre la sociedad, los órganos de representación ciudadana y los responsables.

Título X

Medios de Impugnación

Capítulo I

Del Recurso de Revisión ante el Instituto y los Organismos Garantes

Recurso de revisión y plazo para su interposición

Artículo 93. El titular, por sí mismo o a través de su representante, o bien, o aquellos individuos que ejerzan los derechos ARCO de personas fallecidas, podrán interponer un recurso de revisión ante el Instituto o, en su caso, los organismos garantes o la Unidad de

Transparencia del responsable que haya conocido de la solicitud para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta.

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 o aquellos individuos que ejerzan los derechos ARCO de personas fallecidas podrán interponer el recurso de revisión dentro del año siguiente al que haya vencido el plazo para dar respuesta.

Causales de procedencia del recurso de revisión

Artículo 94. El recurso de revisión procederá cuando menos en los siguientes supuestos:

- I. Se clasifiquen como reservados los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
- II. Se declare la inexistencia de los datos personales;
- III. Se declare la incompetencia por el responsable;
- IV. Se entreguen datos personales incompletos;
- V. Se entreguen datos personales que no correspondan con lo solicitado;
- VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales;
- VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente ley y demás disposiciones que resulten aplicables en la materia;
- VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;
- IX. El titular o el individuo que ejerce los derechos ARCO de una persona fallecida se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;
- X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;
- XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO;
- XII. Se contravenga lo dispuesto por el artículo 53 de la presente ley, o
- XIII. En los demás casos que dispongan las leyes.

Requisitos de la solicitud del recurso de revisión

Artículo 95. Los únicos requisitos exigibles en el escrito de interposición del recurso de revisión serán los siguientes:

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

- II. El nombre del titular que recurre o de su representante legal y, en su caso, del tercero interesado, así como el domicilio o medio que señale para recibir notificaciones;
- III. 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. El acto que se recurre y los puntos petitorios;
- V. En su caso, copia de la respuesta que se impugna y de la notificación correspondiente, y
- VI. Los documentos que acrediten la identidad del titular, y en su caso, la personalidad e identidad de su representante.

Lo anterior, sin perjuicio de aquellos otros elementos potestativos que en las leyes federal, estatales y del Distrito Federal se consideren pertinentes.

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.

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

Conciliación

Artículo 96. 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.

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.

La ley federal y las leyes de los Estados y del Distrito Federal que en la materia resulten aplicables para el cumplimiento de la presente ley, deberán desarrollar la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere este artículo.

Plazo para la resolución del recurso de revisión

Artículo 97. El Instituto y los organismos garantes resolverán el recurso de revisión en un plazo que no podrá exceder de cuarenta días, contados a partir de la admisión del mismo, en los términos que establezca la ley aplicable de la materia, el cual podrá ampliarse hasta por veinte días por una sola vez.

Resolución del recurso de revisión

Artículo 98. Los Organismos garantes resolverán el recurso de revisión conforme a lo siguiente:

- I. Interpuesto el recurso de revisión, el Presidente del organismo garante lo turnará al Comisionado ponente que corresponda, quien deberá proceder a su análisis para que decrete su admisión o su desechamiento;
- II. Admitido el recurso de revisión, el Comisionado ponente deberá integrar un Expediente y ponerlo a disposición de las partes, para que, en un plazo máximo de siete días, manifiesten lo que a su derecho convenga;
- III. Dentro del plazo mencionado en la fracción II del presente artículo, las partes podrán ofrecer todo tipo de pruebas o alegatos excepto la confesional por parte de los sujetos obligados y aquéllas que sean contrarias a derecho;
- IV. El Comisionado ponente podrá determinar la celebración de audiencias con las partes durante la sustanciación del recurso de revisión;
- V. Concluido el plazo señalado en la fracción II del presente artículo, el Comisionado ponente procederá a decretar el cierre de instrucción;
- VI. El organismo garante no estará obligado a atender la información remitida por el sujeto obligado una vez decretado el cierre de instrucción, y
- VII. Decretado el cierre de instrucción, el Expediente pasará a resolución, en un plazo que no podrá exceder de veinte días.

Suplencia de la queja del titular

Artículo 99. 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, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones.

Requerimiento de información al titular

Artículo 100. Si en el escrito de interposición del recurso de revisión el titular no cumple con alguno de los requisitos previstos en el artículo 96 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.

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.

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.

Resolución del recurso de revisión

Artículo 101. Las resoluciones del Instituto o, en su caso, de los organismos garantes podrán:

- I. Sobreseer o desechar el recurso de revisión por improcedente;
- II. Confirmar la respuesta del responsable;
- III. Revocar o modificar la respuesta del responsable, u
- IV. Ordenar la entrega de los datos personales, en caso de omisión del responsable.

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.

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

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 desechamiento del recurso de revisión

Artículo 102. El recurso de revisión podrá ser desechado por improcedente cuando:

- I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 94 de la presente ley;
- II. El Instituto o, en su caso, los organismos garantes hayan resuelto anteriormente en definitiva sobre la materia del mismo;
- III. No se actualice alguna de las causales del recurso de revisión previstas en el artículo 95 de la presente ley;
- IV. Se esté tramitando ante el Poder Judicial 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, o
- V. El recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos.
- VI. El titular no desahogue adecuadamente la prevención del requerimiento de información a que se refiere el artículo 100 de la presente ley.

Causales de sobreseimiento del recurso de revisión

Artículo 103. El recurso de revisión solo podrá ser sobreseído cuando:

- I. El recurrente se desista expresamente;

- II. El recurrente fallezca;
- III. Admitido el recurso de revisión, se actualice alguna causal de improcedencia en los términos de la presente ley;
- IV. El responsable modifique o revoque su respuesta de tal manera que el recurso de revisión quede sin materia, al haber proporcionado el acceso, o haya procedido a la corrección o cancelación solicitada.
- V. Quede sin materia el recurso de revisión.

Plazo de notificación de las resoluciones

Artículo 104. El Instituto y los organismos garantes deberán notificar a las partes y publicar las resoluciones, a más tardar, al tercer día siguiente de su aprobación.

Impugnación de las resoluciones

Artículo 105. Las resoluciones del Instituto serán vinculantes, definitivas e inatacables para los responsables. Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación.

Los titulares podrán impugnar las resoluciones de los recursos de revisión de los organismos garantes ante el Instituto, a través del recurso de inconformidad previsto en el siguiente Capítulo.

Remisión a leyes secundarias

Artículo 106. La ley federal y las leyes de los Estados y del Distrito Federal que en la materia resulten aplicables para el cumplimiento de la presente Ley, deberán desarrollar la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere el presente Capítulo.

Capítulo II Del Recurso de Inconformidad ante el Instituto

Recurso de inconformidad y plazo

Artículo 107. El titular, por sí mismo o a través de su representante, o el individuo que ejerza los derechos ARCO de una persona fallecida podrán impugnar la resolución del recurso de revisión emitido por el organismo garante ante el Instituto, mediante el recurso de inconformidad.

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.

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 del recurso de inconformidad

Artículo 108. El recurso de inconformidad procederá contra la resolución que:

- I. Reserve los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
- II. Determine la inexistencia de datos personales, o
- III. Declare la negativa de datos personales, es decir:
 - a) Se entreguen datos personales incompletos;
 - b) Se entreguen datos personales que no correspondan con los solicitados;
 - c) Se niegue el acceso, rectificación, cancelación u oposición de datos personales;
 - d) 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 de los datos personales, o
 - f) Se oriente a un trámite específico que contravenga lo dispuesto por el artículo 53 de la presente ley.

Requisitos de la solicitud para interponer el recurso de inconformidad

Artículo 109. Los únicos requisitos exigibles e indispensables en el escrito de interposición del recurso de inconformidad son:

- I. El responsable ante la cual se presentó la solicitud para el ejercicio de los derechos ARCO;
- II. El organismo garante que emitió la resolución impugnada;
- III. El nombre del titular que recurre o su representante legal y, en su caso, del tercero interesado, así como su domicilio o el medio que señale para recibir notificaciones;
- IV. La fecha en que fue notificada la resolución al titular;
- V. El acto que se recurre y los puntos petitorios;
- VI. En su caso, copia de la resolución que se impugna y de la notificación correspondiente, y
- VII. Los documentos que acrediten la identidad del titular, y en su caso, la personalidad e identidad de su representante.

El promovente podrá acompañar su escrito con las pruebas y demás elementos que considere procedentes someter a juicio del Instituto, sin perjuicio de aquellos otros elementos potestativos que en la ley federal y de las entidades federativas se consideren pertinentes.

Plazo para resolver el recurso de inconformidad

Artículo 110. 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 período igual.

Suplencia de la queja del titular

Artículo 111. Durante el procedimiento a que se refiere el presente Capítulo, el Instituto deberá aplicar la suplencia de la queja a favor del titular, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones.

Requerimiento de información al titular

Artículo 112. Si en el escrito de interposición del recurso de inconformidad el titular no cumple con alguno de los requisitos previstos en el artículo 107 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.

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 inconformidad.

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.

Resolución del recurso de inconformidad

Artículo 113. Las resoluciones del Instituto podrán:

- I. Sobreseer o desechar el recurso de inconformidad;
- II. Confirmar la resolución del organismo garante;
- III. Revocar o modificar la resolución del organismo garante, o
- IV. Ordenar la entrega de los datos personales, en caso de omisión del responsable.

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.

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

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.

Las medidas de apremio y las sanciones 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 desechamiento del recurso de inconformidad

Artículo 114. El recurso de inconformidad podrá ser desechado por improcedente cuando:

- I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 111 de la presente ley;
- II. El Instituto anteriormente haya resuelto en definitiva sobre la materia del mismo;
- III. No se actualicen las causales de procedencia del recurso de inconformidad, previstas en el artículo 112 de la presente ley;
- III. 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
- IV. El inconforme amplíe su solicitud en el recurso de inconformidad, únicamente respecto de los nuevos contenidos.

Causales de sobreseimiento del recurso de inconformidad

Artículo 115. El recurso de inconformidad solo podrá ser sobreseído cuando:

- I. El recurrente se desista expresamente;
- II. El recurrente fallezca;
- III. El organismo garante modifique o revoque su respuesta de tal manera que el recurso de inconformidad quede sin materia, o
- IV. Admitido el recurso se actualice alguna causal de improcedencia en los términos de la presente ley.

Efecto de la resolución

Artículo 116. 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.

Las leyes de los Estados y del Distrito Federal que en la materia resulten aplicables para el cumplimiento de la presente ley, deberán desarrollar la forma, términos, plazos y procedimientos que regirán la actuación de los organismos garantes relacionada con la emisión de una nueva resolución a que se refiere el párrafo anterior, el cumplimiento de ésta, y en su caso, con la imposición de medidas de apremio a que se refiere el Título XII, Capítulo I de la presente ley.

Cumplimiento de la resolución

Artículo 117. Los sujetos obligados, a través de la Unidad de Transparencia, darán estricto cumplimiento a las resoluciones de los Organismos garantes y deberán informar a estos sobre su cumplimiento.

Excepcionalmente, considerando las circunstancias especiales del caso, los sujetos obligados podrán solicitar a los Organismos garantes, de manera fundada y motivada, una ampliación del plazo para el cumplimiento de la resolución.

Dicha solicitud deberá presentarse, a más tardar, dentro de los primeros tres días del plazo otorgado para el cumplimiento, a efecto de que los Organismos garantes resuelvan sobre la procedencia de la misma dentro de los cinco días siguientes.

Artículo 118. Transcurrido el plazo señalado en el artículo anterior, el sujeto obligado deberá informar al organismo garante sobre el cumplimiento de la resolución.

El organismo garante verificará de oficio la calidad del cumplimiento de la resolución, y, a más tardar al día siguiente de recibir el informe, dará vista al recurrente para que, dentro de los cinco días siguientes, manifieste lo que a su derecho convenga. Si dentro del plazo señalado el recurrente manifiesta que el cumplimiento no corresponde a lo ordenado por el organismo garante, deberá expresar las causas específicas por las cuales así lo considera.

Artículo 119. El organismo garante deberá pronunciarse, en un plazo no mayor a cinco días, sobre todas las causas que el recurrente manifieste así como del resultado de la verificación realizada. Si el organismo garante considera que se dio cumplimiento a la resolución, emitirá un acuerdo de cumplimiento y se ordenará el archivo del expediente. En caso contrario, el organismo garante:

- I. Emitirá un acuerdo de incumplimiento;
- II. Notificará al superior jerárquico del responsable de dar cumplimiento, para el efecto de que, en un plazo no mayor a cinco días, se dé cumplimiento a la resolución, y
- III. Determinará las medidas de apremio o sanciones, según corresponda, que deberán imponerse o las acciones procedentes que deberán aplicarse, de conformidad con lo señalado en el Título XII de la presente ley.

Remisión a leyes secundarias

Artículo 120. La ley federal que en la materia resulte aplicable para el cumplimiento de la presente Ley, deberá desarrollar la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere el presente Capítulo.

Impugnación de las resoluciones

Artículo 121. Las resoluciones del Instituto serán vinculantes, definitivas e inatacables para el organismo garante y el responsable de que se trate. Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación.

Capítulo III De la Atracción de los Recursos de Revisión

Facultad de atracción

Artículo 122. Para efectos de la presente ley, el Instituto de oficio o a petición fundada de los organismos garantes podrá ejercer la facultad de atracción para conocer de aquellos recursos de revisión 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 la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

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 en materia de transparencia y acceso a la información pública en materia de protección de datos personales se deberán considerar los siguientes factores:

- I. La finalidad del tratamiento de los datos personales;
- II. El número y tipo de titulares involucrados en el tratamiento de datos personales llevado a cabo por el responsable;
- III. La sensibilidad de los datos personales tratados;
- IV. Las posibles consecuencias que se derivarían de un tratamiento indebido o indiscriminado de datos personales, y
- V. 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.

Capítulo IV De los criterios de interpretación

Facultad para emitir criterios de interpretación

Artículo 123. Una vez que hayan causado ejecutoria las resoluciones dictadas con motivo de los recursos de revisión, el Instituto, podrá emitir los criterios de interpretación que estimen 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.

Título XI
Facultad de Verificación del Instituto y los Organismos Garantes

Capítulo Único
Del Procedimiento de Verificación

Facultades de vigilancia y verificación del Instituto y los organismos garantes

Artículo 124. El Instituto y los organismos garantes, en el ámbito de sus respectivas competencias, 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.

En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los organismos garantes estarán dotados de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo, así como estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.

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.

Causales de un procedimiento de verificación

Artículo 125. La verificación podrá iniciarse:

- I. De oficio cuando el Instituto o los organismos garantes cuenten con indicios que hagan presumir fundada y motivadamente la existencia de violaciones a las leyes correspondientes, o
- II. 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.

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

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 la orden de verificación respectiva.

Requisitos de la denuncia

Artículo 126. Para la presentación de una denuncia no podrán solicitarse mayores requisitos que los que a continuación se describen:

- I. El nombre de la persona que denuncia o, en su caso, de su representante;
- II. El domicilio o medio para recibir notificaciones de la persona que denuncia;
- III. La relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho;
- IV. El responsable denunciado y su domicilio o, en su caso, los datos para su identificación y/o ubicación, y
- V. La firma del denunciante, o en su caso, de su representante. En caso de no saber firmar, bastará la huella digital.

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.

Inicio de una verificación

Artículo 127. 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.

El procedimiento de verificación deberá tener una duración máxima de cincuenta días, el cual podrá ampliarse por un periodo igual por una sola vez.

Medidas precautorias

Artículo 128. Si derivado del desarrollo del procedimiento de verificación el Instituto o los organismos garantes advierten la necesidad de dictar medidas precautorias, éstos podrán decretarlas en términos de lo que establezcan las leyes respectivas.

Conclusión del procedimiento de verificación

Artículo 129. El procedimiento de verificación concluirá con la resolución que emita el Instituto o los organismos garantes, en la cual, en su caso, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.

Auditorías voluntarias

Artículo 130. 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.

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.

Remisión a leyes secundarias

Artículo 131. La ley federal y las leyes de los Estados y del Distrito Federal que en la materia resulten aplicables para el cumplimiento de la presente ley, deberán desarrollar la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere el presente Capítulo.

Título XII

Medidas de Apremio, Responsabilidades y Sanciones

Capítulo I

De las Medidas de Apremio

Cumplimiento de las resoluciones

Artículo 132. Para el cumplimiento de las resoluciones recaída a los recursos de revisión emitidas por el Instituto o los organismos garantes, según corresponda, el responsable y éstos deberán observar lo dispuesto en el Capítulo VI del Título VII de la Ley General de Transparencia y Acceso a la Información Pública.

Imposición de medidas de apremio

Artículo 133. El Instituto y los organismos garantes podrán imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus resoluciones:

- I. La amonestación, o
- II. La multa, de ciento cincuenta hasta mil quinientas veces el salario mínimo general vigente en el área geográfica de que se trate.

La ley federal y las de los Estados y del Distrito Federal establecerán los criterios para calificar las medidas de apremio, conforme a la gravedad de la falta y, en su caso, las condiciones económicas del infractor y la reincidencia.

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.

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 144 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.

Incumplimiento de la resolución

Artículo 134. 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 tres días lo obligue a cumplir sin demora. De persistir el incumplimiento, se aplicarán sobre aquél las medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista a la autoridad competente en materia de responsabilidades.

Aplicación de las medidas de apremio

Artículo 135. 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.

Criterios para la determinación de medidas de apremio

Artículo 136. Para la determinación de las medidas de apremio, el Instituto y los organismos garantes deberán considerar los criterios previstos en las leyes que resulten aplicables en la materia.

Autoridad competente para hacer efectivas las multas

Artículo 137. Las multas que fijen el Instituto y los organismos garantes se harán efectivas ante el Servicio de Administración Tributaria o las Secretarías de Finanzas de las Entidades Federativas, según corresponda, a través de los procedimientos que las leyes establezcan.

Remisión a leyes secundarias

Artículo 138. La ley federal, las leyes de los Estados y del Distrito Federal que en la materia resulten aplicables para el cumplimiento de la presente ley deberán establecer los mecanismos y plazos para la notificación y ejecución al Instituto y los organismos garantes de las medidas de apremio que se apliquen en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio.

Remisión a leyes que prevén medidas de apremio

Artículo 139. Además de las medidas de apremio previstas en el presente Capítulo, las leyes de la materia podrán establecer aquéllas otras que consideren necesarias.

Capítulo II

De las Responsabilidades Administrativas de los Servidores Públicos y Sanciones

Causales de responsabilidad administrativa de los servidores públicos

Artículo 140. Serán causas de responsabilidad administrativa de los servidores públicos por incumplimiento de las obligaciones establecidas en la presente ley las siguientes:

- I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
- II. Incumplir, con dolo, los plazos de atención previstos en la presente ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
- III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
- IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente ley;
- V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refieren los artículos 20 y 21 de la presente ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia, o bien, no poner a disposición del titular el aviso de privacidad en los términos que señala la presente ley y demás disposiciones que resulten aplicables;
- VI. Aplicar medidas compensatorias en contravención de los criterios que para tales fines establezca el Instituto;
- VII. Declarar dolosamente la inexistencia de datos personales cuando éstos existan total o parcialmente en los archivos del responsable;
- VIII. Declarar dolosamente la incompetencia del responsable, teniendo atribuciones en la materia;
- IX. Reservar con dolo 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;
- X. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente ley;
- XI. No establecer las medidas de seguridad en los términos que establecen los artículos 37, 38 y 39 de la presente ley;
- XII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 37, 38 y 39 de la presente ley;
- XIII. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente ley;
- XIV. Obstruir los actos de verificación de la autoridad;
- XV. No atender las medidas precautorias establecidas por el Instituto o los organismos garantes;

- XVI. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos;
- XVII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente ley;
- XVIII. No acatar las resoluciones emitidas por el Instituto y los organismos garantes;
- XIX. No cumplir con las disposiciones previstas en los artículos 58 y 62 de la presente ley;
- XX. Omitir la inscripción de los sistemas de datos personales en su posesión en el Registro;
- XXI. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 84, fracción V de la presente ley, o bien, entregar el mismo de manera extemporánea, y
- XXII. Tratar datos personales en aquellos casos en que sea necesario presentar la manifestación de impacto a la privacidad, de conformidad con lo previsto en la presente ley y demás normativa aplicable

Las causas de responsabilidad previstas en las fracciones I, II, IV, VII, VIII, IX, XIV, XV, XVII, XVIII, XIX y XXII 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.

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.

Aplicación de la legislación en materia de responsabilidad administrativa de los servidores públicos

Artículo 141. Las conductas a que se refiere el artículo anterior serán sancionadas por el Instituto y los organismos garantes, según corresponda, y, en su caso, conforme a su competencia darán vista a la autoridad competente para que imponga o ejecute la sanción.

Procedencia de responsabilidades del orden civil o penal

Artículo 142. Las responsabilidades administrativas a que se refiere este Capítulo, son independientes de las del orden civil o penal que procedan.

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.

Para tales efectos, el Instituto y los organismos garantes podrán denunciar ante las autoridades competentes cualquier acto u omisión violatorio de la presente ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

Régimen de partidos políticos y fideicomisos públicos

Artículo 143. Ante incumplimientos por parte de los partidos políticos, el Instituto y el organismo garante competente dará vista, según corresponda, al Instituto Nacional Electoral o a los organismos públicos locales electorales de las Entidades Federativas y el Distrito Federal competentes, para que resuelvan lo conducente, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.

En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto o el 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.

Remisión de expediente a autoridades competentes

Artículo 144. En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto o el organismo garante deberán 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.

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.

TRANSITORIOS

PRIMERO. La presente Ley entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO. A la entrada en vigor de la presente Ley quedarán abrogadas todas aquellas disposiciones que contravengan los principios, bases y derechos reconocidos en ésta.

TERCERO. La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y las leyes vigentes de los Estados y del Distrito Federal en materia de protección de datos personales, deberán ajustarse a las disposiciones previstas en la presente Ley en un plazo de un año siguiente contado a partir de la entrada en vigor de la presente Ley.

En caso de que el Congreso de la Unión, las legislaturas estatales o la Asamblea del Distrito Federal omitan total o parcialmente realizar las adecuaciones legislativas a que haya lugar, en el plazo establecido en el párrafo anterior, resultará aplicable de manera directa la presente Ley, con la posibilidad de seguir aplicando de manera supletoria las

leyes preexistentes en todo aquello que no se oponga a la misma, hasta en tanto no se cumpla la condición impuesta en el presente artículo.

CUARTO. El Registro Nacional de Protección de Datos a que se refiere la presente Ley deberá crearse dentro de los dos años a partir de la entrada en vigor de la presente Ley. Para su creación deberán preverse los recursos suficientes en el Presupuesto de Egresos de la Federación.

QUINTO. El Gobierno Federal deberá hacer las provisiones presupuestales necesarias para la operación de la presente Ley y establecer una partida presupuestal específica en el Presupuesto de Egresos de la Federación para el siguiente ejercicio fiscal a su entrada en vigor.

SEXTO. Se derogan todas aquellas disposiciones en materia de protección de datos personales, de carácter federal, estatal y municipal, que contravengan lo dispuesto por la presente Ley.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

México D.F. a 30 de abril de 2015
Salón de Sesiones del Pleno del Senado de la República



Sen. Laura Angélica Rojas Hernández

Sen. Alejandro Encinas Rodríguez

Sen. Cristina Díaz Salazar

Sen. Fernando Yunes Márquez

Sen. María Marcela Torres Peimbert

Sen. Zoé Robledo Aburto

Sen. Héctor Larios Córdova

Sen. Armando Ríos Piter

Sen. Isidro Pedraza Chávez

Sen. Pablo Escudero Morales