AÑO: 2015 EXPEDIENTE: 9239/LXXIII

H. Congreso del Estado de Nuevo León

LXXIII Legislatura

PROMOVENTE: LIC. SERGIO MARES MORAN, COMISIONADO PRESDIENTE; LIC. SERGIO ANTONIO MONCAYO GONZALEZ, COMISIONADO VOCAL E ING. JUAN DE DIOS VILLARREAL GONZALEZ, COMISIONADO VOCAL DE LA COMISION DE TRANSPARENCIA Y ACCESO A LA INFORMACION DEL ESTADO DE NUEVO LEON.

ASUNTO RELACIONADO: ESCRITO MEDIANTE EL CUAL PRESENTAN INICIATIVA PARA LA CREACION DE LA LEY DE PROTECCION DE DATOS PERSONALES PARA EL ESTADO DE NUEVO LEON, LA CUAL CONSTA DE 112 ARTICULOS Y 8 ARTICULOS TRANSITORIOS.

INICIADO EN SESIÓN: 11 DE FEBRERO DE 2015

SE TURNÓ A LA (S) COMISIÓN (ES): Legislación y Puntos Constitucionales

Lic. Mario Treviño Martínez

Oficial Mayor

COMISIÓN DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN DEL ESTADO DE NUEVO LEÓN ®

HONORABLE CONGRESO DEL ESTADO DE NUEVO LEÓN

LXXIII LEGISLATURA.

PRESENTE.-

SERGIO MARES MORÁN, SERGIO ANTONIO MONCAYO GONZÁLEZ, JUAN DE DIOS VILLARREAL GONZALEZ Y MARÍA EUGENIA PÉREZ EIMBCKE, Comisionados integrantes de la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León; con fundamento en lo dispuesto por los artículos 63 y 68 de la Constitución Política del Estado Libre y Soberano de Nuevo León, así como los diversos 102, 103 y demás relativos del Reglamento para el Gobierno Interior del Congreso del Estado de Nuevo León, nos permitimos someter a la consideración de esta Honorable Legislatura LXXIII, iniciativa para la creación de la Ley de Protección de Datos Personales para el Estado de Nuevo León, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

El derecho a la protección de los datos personales se encuentra contemplado en la Ley de Transparencia y Acceso a la Información del Estado, en el Título Segundo de la mencionada Ley; pero el acceso a la información pública y la protección de datos personales pueden ser considerados derechos en conflicto, por lo que es conveniente contar con una ley específica para cada materia y así en su momento poder realizar la ponderación respectiva, sobre cual derecho prevalecerá sobre otro, cuando así lo amerite el caso y se demuestre el porqué deberá

prevalecer los intereses generales u otros particulares sobre el poder de decisión que dispone cada persona sobre su propia privacidad soslayando el condicionamiento del consentimiento previo para tratar los datos.

México tiene la peculiaridad de que su régimen regulador de la protección de datos ha surgido de las normas referentes al derecho de acceso a la información pública. La reforma a la Constitución en el 2009, incluye el derecho fundamental a la protección de datos personales, lo que coloca a México en la lista de países que han constitucionalizado el tema. El texto, incluido en el artículo 16 de la Constitución Mexicana por decreto publicado el primero de junio del 2009, prevé 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 pública o para proteger los derechos e terceros".

Estos cambios constitucionales apuntan a una futura autonomía legislativa de la protección de datos personales. La cual, en la actualidad se encuentra en la Ley de Transparencia y Acceso a la Información del Estado.

De lo anterior se desprende el mencionar que el Derecho a la Protección de Datos Personales previene el uso indebido e indiscriminado de los datos personales y tiene por objeto primordial garantizar y proteger, en lo que concierne

al tratamiento de los datos personales, las libertades y derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal.

Se trata fundamentalmente de proteger a las personas físicas identificadas o identificables del uso indebido de cualquier información o dato personal que les afecte. Lo cual se configura normativamente como un derecho nuevo de tercera generación, distinto a los demás, motivados por el límite al uso de la informática y las nuevas tecnologías de la información.

Ha de entenderse que el derecho a la protección del dato personal se considera de tercera generación, ya que debemos de contemplar las generaciones o fases de derechos humanos, que constituyen la evolución del reconocimiento de nuevos derechos que intentan dar respuesta a las nuevas necesidades humanas en función de las amenazas o nuevas situaciones que surgen.

Así se han reconocido tres generaciones de derechos que han correspondido a un momento ideológico y social, con características propias y rasgos diferenciados.

Para comprender y entender cada uno, me permitiré comentar lo siguiente: la primera generación de derechos, propia del sentimiento individualista y las revoluciones burguesas del siglo XVIII, ha quedado marcada por las libertades individuales, lo que ha constituido los derechos de defensa de la persona, cuya exigencia consistía en la no injerencia de los poderes públicos en la esfera privada

de las personas. En esta fase se configuraron una serie de derechos relativos al aislamiento, tal como lo fue el derecho al honor, a la vida, a la integridad personal, así como el propio reconocimiento a la intimidad de la persona. Derecho que hoy, como consecuencia del desarrollo tecnológico y las nuevas formas de comunicación e información, ha sido necesario reformular en su alcance y contenido.

Una segunda generación de derechos humanos, nace en las luchas sociales del siglo XIX. Los movimientos reivindicatorios evidenciaron la necesidad de completar el catálogo de derechos y libertades de la primera generación, con una segunda generación de derechos económicos, sociales y culturales. Contemplando así mismo los derechos de participación. En la tercera generación, que es en la que nos encontramos inmersa, los derechos fundamentales, con una visión solidaria, tratan de completar los anteriores derechos, ante la nueva realidad tecnológica y la contaminación de todo tipo, que surge, con valores como la paz, el medio ambiente, la calidad de vida, el control de la manipulación genética, la "libertad informática", etc.

La Protección de Datos de carácter personal supone, pues, el nacimiento de un derecho de tercera generación que ampara a los ciudadanos contra la posible utilización por terceros, no autorizada, de sus datos personales.

Este derecho ha sido recogido en todas las legislaciones de transparencia y acceso a la información de México. Sin embargo su importancia y necesidad, hace

palpable y latente la necesidad de un marco jurídico específico en la materia, que proteja debidamente el tratamiento de los datos de carácter personal en nuestro Estado, ya que los datos personales que tiene cada una de las autoridades, no les pertenecen, son simples poseedores y guardianes de dicha información, para cumplir con la finalidad para la cual se les proporcionaron.

Este derecho que es conocido como "autodeterminación informativa", marca un hito en la defensa de los derechos de la persona a preservar sus datos personales, permitiendo la libre decisión y disposición sobre sus datos personales y sus fines. Señalando que la proliferación de centros de tratamiento de datos permite, gracias a los avances tecnológicos producir un perfil de la personalidad, incluso en el ámbito de su intimidad, que convierte al ciudadano en "hombre de cristal". Lo que da lugar al nacimiento de la propuesta de Ley de Protección de Datos en posesión de los Sujetos Obligados.

Quienes traten datos de carácter personal, ya sean particulares o autoridades, que son las que nos competen, tienen la obligación de respetar el Derecho de los titulares, a que sus datos sean tratados leal y legalmente, pues como titulares de esos datos tienen derecho a ejercer un control y un poder de decisión sobre cuándo, dónde, cómo y por quién son tratados. Control que pueden exigir a través del ordenamiento jurídico, ante la actual Comisión de Transparencia y Acceso a la Información del Estado, y que en la iniciativa de la nueva Ley de Transparencia se propone llamar Instituto de Transparencia, Acceso a la

Información y Protección de Datos Personales en el Estado, como autoridad autónoma encargada de su vigilancia y cumplimiento.

Así los principios, derechos y procedimientos necesarios para el desarrollo y aplicación efectiva de este Derecho Fundamental a la Protección de Datos se ven protegidos o garantizados por nuestros derechos de Acceso, Rectificación, Cancelación y Oposición del tratamiento de los datos personales en posesión de los sujetos obligados.

Por lo cual, el respeto al derecho fundamental a la protección de datos y su aplicación práctica a través de los principios, derechos y procedimientos conlleva una serie de obligaciones para quienes traten datos personales, por lo tanto, todos los sujetos obligados están sujetos a una serie de obligaciones, cuyo incumplimiento es objeto de sanciones pecuniarias para aquel que infrinja los supuestos establecidos en la presente iniciativa de ley.

Indudablemente el uso de las nuevas tecnologías de la información en el campo de la informática ha traído consigo situaciones y realidades que hace algunos años eran imposibles e inimaginables. Hoy la realidad es que en cuestión de segundos es posible obtener, almacenar y someter a tratamiento una infinidad de datos personales, lo cual facilita y crea condiciones favorables para el trabajo realizado.

Así mismo, el uso indebido de los datos personales, puede tener consecuencias graves para una persona, las cuales pueden ir desde la provocación de actos de molestia al titular del dato, consistentes de envío de información no solicitada; pasando por actos de discriminación, toda vez que mediante el cruce de información de una persona, se puede configurar un perfil respecto de sus gustos, creencias, afinidades o que decir de su estado de salud física o mental, que pueden influir negativamente al momento de solicitar un servicio o adquiera un bien; hasta la comisión de delitos graves como perdida de patrimonio, secuestro o el robo de identidad.

El uso perverso de la información de carácter personal puede crear problemas muy serios que convierten a la persona en un ser frágil que vive ante una amenaza latente de ser observado en forma permanente.

Por lo cual, se debe contemplar que todos los sujetos obligados que tratan datos de carácter personal tienen, correlativa y necesariamente pues, que cumplir deberes jurídicos que permitan hacer efectivo a las personas afectadas el poder de control y disposición sobre sus datos personales.

De tal forma, que los sujetos obligados cuando lleven a cabo el tratamiento de los datos de carácter personal, tienen que respetar el derecho que los ciudadanos tienen, de que sus datos personales sean tratados confidencial y legalmente, pues como titulares de sus datos personales tienen derecho a ejercer un control y poder de decisión sobre cuándo, dónde, cómo y por quien son tratados.

Por lo tanto, la Protección de datos Personales es un derecho frente al Estado y frente a los poderes públicos, a los que exige un respeto a una esfera personal, a los datos personales, que obliga a cumplir los principios de protección de datos, que no son otra cosa que obligaciones de hacer y no hacer, de los sujetos obligados en relación al tratamiento de las bases de datos en su posesión.

Por lo cual, debe entenderse que el derecho a la protección de datos garantiza a la persona un poder de autocontrol sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer, distintos ambos radicalmente del Derecho a la Intimidad, cuyo origen hay que buscarlo cuando se construye el Estado liberal y aparece la burguesía y el individualismo.

Históricamente lo íntimo y lo privado se han ido desarrollando a costa de lo público. La vida íntima y privada ha ido creciendo a medida que se ha ido limitando el ansia expansionista del poder político. Así, de la confrontación de la idea de libertad frente al omnipresente poder público, aparece el derecho a la intimidad como un conjunto de poderes y facultades para garantizar la exclusión del Estado en el ámbito más secreto del individuo. Para los liberales, "el disfrute de la libertad está intrínsecamente unido a la existencia de ese dominio privado. La idea de intimidad surge ante la necesidad del individualismo moderno, de la búsqueda de la soledad y del retiro, como privilegio de clase.

El derecho a la intimidad se define por primera vez en 1890 por los juristas norteamericanos SAMUEL D. WARREN Y LOUIS D. BRANDEIS como el derecho a estar solo o a no ser molestado en su monografía "The Rigt to privacy". Pretendiendo paliar las continuas intromisiones de la prensa en la vida privada de las personas. Para conseguir su objetivo estudian las normas y principios de derecho ya existentes en el Common law llegando a la conclusión de que "el derecho a la intimidad se caracteriza por el rechazo a toda intromisión no consentida; es decir, el derecho a la intimidad se configurará como un típico derecho de "no interferencia", con los siguientes limites en lo que es público o de interés general.

El derecho a la protección de datos (autodeterminación informativa) tiene un contenido y ámbito diferente.

El nuevo derecho fundamental a la protección de datos, la razón histórica de la aparición de este nuevo derecho se encuentra en el veloz desarrollo de las nuevas tecnologías en los últimos años, donde la informática aparece como una herramienta al servicio de la humanidad pero que como herramienta poderosa puede ser usada de forma negativa.

El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero puede afectar a

sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, sino los datos de carácter personal que ampara.

Por lo tanto, es de entenderse que los principios de transparencia y publicidad son esenciales para el correcto desarrollo de la democracia. No obstante, la divulgación de la identidad y posibles datos considerados como sensibles, deben protegerse. Por lo que se debe de entender, que la transparencia y la publicidad inherente a la actuación de los sujetos obligados en sus relaciones con los ciudadanos, así como el acceso a la información pública, que son exigencias constitucionalmente reconocidas como pilares del sistema democrático, deben acarrear la necesaria pero también la mínima divulgación de datos personales.

La presente iniciativa está compuesta de diez títulos, entre los cuales se establece en el Título Primero que el objeto de la Ley es la Protección de los datos personales contenidos en las bases de datos en posesión de los sujetos obligado, con la finalidad de garantizar el derecho al honor, imagen y vida privada de los ciudadanos.

En el cual, también se definen conceptos elementales para la aplicación de la presente iniciativa de Ley.

En el Título Segundo, se encuentran comprendidos los principios por los cuales se rige el derecho a la protección del dato personal, los cuales se traducen en

obligaciones de hacer y de no hacer de los sujetos obligados frente al tratamiento de las bases de datos que tienen en su posesión.

Los principios de la protección de datos son la base de tan importante Derecho, por lo cual es importante que estén debidamente definidos cada uno, puesto que de ellos emanan prácticamente todas las obligaciones.

La presente iniciativa contempla los principios de consentimiento, información previa, finalidad, licitud, calidad de la información, confidencialidad, seguridad, proporcionalidad, máxima privacidad, responsabilidad e irrenunciablidad, así como garantizar los derechos de acceso, rectificación, cancelación y oposición de datos personales.

El principio de calidad de la información, es muy importante ya que de él se derivan otras obligaciones que han de cumplir y procurar su cumplimiento los sujetos obligados cuando traten datos de carácter personal, especialmente en los casos de las excepciones al consentimiento. Por lo cual para cumplir con el presente principio los datos deberán de responder con veracidad a la situación actual del titular del dato. Deberán ser: exactos, actualizados, completos, adecuados, pertinentes y no excesivos en su tratamiento.

El principio de finalidad contempla que los datos recabados legalmente tienen que ser apropiados para el fin para el que fueron almacenados y obtenidos.

Por lo tanto, los datos personales deben ir de acuerdo con el fin para el que fueron obtenidos, lo que se conoce como adecuación al fin, junto con la cancelación y rectificación de oficio en determinados supuestos que se especifican en la presente iniciativa.

Hay que señalar que el principio de finalidad limita los usos lícitos de los datos personales. Es el elemento esencial que permitirá encontrar una solución a los problemas jurídicos que se plantean en cuanto a la protección de la privacidad en los casos en que bases de datos de carácter público son accesibles en internet.

Así mismo, nos encontramos ante el principio del consentimiento del titular del dato, considerado el pilar de los principios de protección de datos, el cual se puede resumir "el titular del dato es el único que decide cuándo, dónde y cómo se presentan sus datos al exterior, o se dan a conocer sus datos a terceros" esto es, el titular tiene que otorgar su consentimiento para que se pueda realizar un tratamiento de sus datos de carácter personal desde la primera fase que es la obtención de los mismos. En dicho principio también se prevén excepciones al consentimiento, así como cuando pueden revocar el mismo y que esta revocación sea de una forma sencilla y gratuita. Por lo anterior es considerado el principio esencial ya que es la materialización de la autodeterminación informativa que permite al ciudadano decidir cuándo, dónde, cómo y por quién son tratados sus datos de carácter personal.

Aunado a los anteriores principios nos encontramos con el principio de información previa, es un principio general de protección de datos que nos dice que todo titular tiene derecho a ser informado cuando se le solicitan datos de carácter personal con el fin de que conozca quién, cómo y para qué los va a tratar, así como poder ejercitar, en su caso, los derechos que tiene. Por otro lado, hay que tener en cuenta que, así mismo puede haber ocasiones en las que los datos personales puedan ser recabados de determinadas fuentes que dada su finalidad pueden ser accesibles a cualquiera sin necesidad de contar con el consentimiento de los interesados, es decir, de las conocidas como fuentes de acceso público, las cuales se prevén en la presente iniciativa.

El principio de seguridad es sumamente importante, ya que en el transcurso del tratamiento de los datos, surgen riesgos para los datos de carácter personal, ya provengan de la acción humana o del medio físico en el que estén, que podrían conducir a una vulneración de la intimidad del titular, lo que sería contrario al objeto de la Ley de Transparencia y Acceso a la Información del Estado de Nuevo León y atribución de la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León, la cual es "garantizar y proteger, en lo concerniente al tratamiento de los datos personales". Además, las medidas deben ser cambiantes, adaptándose en cada momento al estado de la tecnología, que es cambiante por su propia naturaleza, a la naturaleza de los datos, no es lo mismo el nombre o la dirección de un individuo que sus datos de salud, y los riesgos a que se encuentran expuestos (no es lo mismo un tratamiento manual a uno automatizado).

Principio de Confidencialidad, se traduce en el deber de secreto, la cual es una obligación general para todos aquellos que traten datos de carácter personal. Es importante destacar que quienes intervengan en cualquier fase del tratamiento, normalmente serán empleados, por los que hay obligación de responder respecto de los perjuicios causados por ellos con ocasión de sus funciones encomendadas.

El principio de proporcionalidad en el tratamiento de los datos de carácter personal se encuentra vinculado a la finalidad, de este modo sólo podrán recabarse aquellos datos que sean necesarios para conseguir los fines que motivan su obtención.

A lo anterior, ha de añadirse que el cumplimiento de la proporcionalidad exige que se opte, de entre los tratamientos que permitan conseguir los fines pretendidos, pro el que menor incidencia tenga en el derecho a la protección del dato. Por lo cual el dato deberá ser adecuado, pertinente y no excesivo de acuerdo a la finalidad para la cual se obtuvo.

El principio de licitud, se refiere a que la obtención de los datos personales sea de acuerdo a fines lícitos, es decir, que tenga que ver con las atribuciones que le confiere una ley y por lo cual corresponden al sujeto obligado que se encuentra obteniendo o recopilando los datos personales del titular, ya sea para brindarle un servicio o bien para llevar a cabo un registro, que alguna ley prevea.

Principio de responsabilidad, en el cual la persona que haya sido designada como responsable, tiene la obligación de velar y responder por el tratamiento de los datos personales que tengan bajo su resguardo, o por aquellos datos que haya comunicado a un encargado o tercero, lo anterior siempre bajo los estándares señalados en la presente iniciativa y por aquellos que establezca el propio sujeto obligado en su documento de seguridad.

Principio de Irrenunciabilidad, en el cual se establece que los datos personales, son irrenunciables, intransferibles, por lo que, no podrán transmitirse, salvo disposición legal o cuando haya mediado el consentimiento del titular del datos. Y por último, en relación a los principios se encuentra el de máxima privacidad, en el cual, el sujeto obligado tendrá que proteger y resguardar la intimidad y privacidad de los datos personales, que se encuentran bajo su resguardo, aún cuando ya no labore para el sujeto obligado.

Posteriormente en el Título Tercero, se contemplan los derechos de los titulares. Para poder conocer los derechos de los titulares de datos de carácter personal, debemos tener presentes los principios que acabamos de mencionar, ya que estos son correlativos a la facultad del ejercicio de los derechos ARCO por el ciudadano que dan efectividad práctica a los mencionados principios. Derechos que al ser independientes, no necesitan ninguna prelación en su ejercicio y pueden ejercerse sin que ninguno de ellos sea requisito previo para el ejercicio de otro.

Por tanto resaltamos que el respeto a los derechos de los titulares implican obligaciones reales para el responsable del sistema, no una mera declaración teórica de intenciones, por tanto exige que se defina un procedimiento dentro de la organización del sujeto obligado, que permita cumplir con las formalidades y prescripciones establecidas para que estos derechos se establezcan y ejerzan.

De esta forma, el sujeto obligado no cumple solamente con tratar los datos personales respetando todos los principios mencionados si no que, además, es necesario que permita y facilite el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición, de la forma como se ha establecido en la presente iniciativa.

Ahora bien, en el Titulo Cuarto, se prevé el tratamiento y registro de datos personales, en el cual se establece, que el derecho a la protección de los datos personales será para sistemas de bases de datos automatizados o físicos. Los cuales, son conjuntos organizados de archivos que como su nombre lo indica, contienen datos de una forma organizada y los hace plenamente identificables. Se prevé que las bases de datos que se encuentran en posesión de los sujetos obligados deban registrarlas ante la Comisión de Transparencia y demás información que deberán hacer llegar a la misma, para poder tener esa información disponible para el ciudadano.

Igualmente, en el presente Título se abordó el tema de la video vigilancia , en la cual sabemos que es una práctica muy extendida en nuestra sociedad, lo cual

nos da como resultado, una sociedad vigilada, fruto probablemente de las mismas demandas de los ciudadanos y de la exigencia social de garantizar una mayor seguridad, la video vigilancia, generalmente persigue, el garantizar la seguridad de los bienes y las personas, verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales y responder a las demandas de los ciudadanos que quieren obtener información visual de un hecho acontecido.

Por lo cual, la utilización de los medios técnicos para la vigilancia repercute sobre los derechos de las personas, lo que obliga a fijar garantías.

La video vigilancia permite la captación, y en su caso la grabación, de información personal en forma de imágenes. Cuando su uso afecta a personas identificadas o identificables está información constituye un dato de carácter personal. Como se considera un medio particularmente invasivo y por ello resulta necesario que se encuentre regulado en el presente proyecto de Ley.

En el mismo orden de ideas, nos encontramos en el Título Quinto, en el cual se contempla los requisitos y excepciones para poder realizar transmisiones de las bases de datos personales en posesión de los sujetos obligados, respetando en todo momento la garantía del ciudadano a proteger su información de carácter personal. La transmisión de datos es el tratamiento de datos en la cual se supone su revelación a una persona distinta del interesado.

La transmisión de datos constituye, sin duda, el mayor de los peligros a que se puede exponer a los titulares de los datos porque puede conllevar la pérdida del control y de los datos, su utilización para finalidades distintas a las que motivaron su tratamiento y la elaboración de un perfil del individuo que ni él mismo conoce. Por eso, la Comisión se preocupa por este tema crucial y se incluye en la presente iniciativa, para que los sujetos obligados al momento de tratar las bases de datos que tienen en su posesión, observen con especial atención el que no se produzca nunca una transmisión de o cesión de datos no consentida o permitida por la ley.

Posteriormente se encuentra en el Título Sexto la seguridad de los datos personales, en el cual se contemplan medidas de seguridad que deberán implementar los sujetos obligados hacia las bases de datos que tienen en su reguardo y los cuales deberán ser en relación al nivel de datos al que pertenezcan, los cuales son los mínimos que deberán implementar para la seguridad de la información de carácter personal. En el mismo apartado se encuentran las obligaciones que deberá cumplir la persona física que sea designado como responsable de las bases de datos que se encuentren en su posesión y resguardo.

Así mismo, en el Título Séptimo se establece los requisitos que debe reunir el documento de seguridad que deberá tener todo sujeto obligado y en el cual se deberán sujetar a lo establecido por el mismo, En dicho documento deberán establecerse las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos. Este apartado regula un aspecto esencial para la tutela del derecho fundamental a la protección de los datos, la seguridad, que

repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todos los sujetos obligados que traten datos personales.

Por lo que respecta en el Título Octavo se establecen las atribuciones como Órgano Garante en relación al derecho de la protección de datos personales, que ya se encontraban en la Ley de Transparencia, pero se sustrajeron de la misma para que se encuentren en la presente iniciativa.

Por mencionar algunas, dentro de sus atribuciones se encuentra la difusión y protección de los datos personales en posesión de los sujetos obligados, el desarrollo, fomento y difusión de análisis, estudios e investigaciones en materia de datos personales, establecimiento de lineamientos que en materia de seguridad en el tratamiento de datos se deben de expedir, emisión de recomendaciones a los sujetos obligados en relación al tratamiento de sus bases de datos, así como conocer y resolver los procedimientos de inconformidad que se presenten, así como imponer las sanciones correspondientes.

Por otro lado, se encuentra en el Título Noveno, el procedimiento que deberán hacer valer el titular del dato, cuando se sienta vulnerado en el tratamiento de sus datos personales.

Finalmente en el Título Décimo, se especifica los supuestos de responsabilidades y sanciones en las cuales podría infringir el responsable en el tratamiento de las bases de datos de los ciudadanos.

Por lo anteriormente expuesto, los principios, derechos y procedimientos necesarios para el desarrollo y aplicación efectiva de este derecho fundamental a la protección de datos, se vislumbra en la presente iniciativa de Ley, ya que los sujetos obligados que traten bases de datos de carácter personal, tendrán la obligación de respetar los principios, derechos y procedimientos que conllevan una serie de obligaciones para todos los responsables y encargados, cuyo incumplimiento es objeto de sanciones.

Así pues, el derecho a la protección de dato adquiere un carácter propio e independiente, cuya justificación radica en la protección que otorga a las personas físicas del tratamiento (automático o no y sus consecuencias) de cualquier clase de datos personales (no solo los considerados sensibles), no consentido ni autorizado. Haciendo de esta forma efectivo el control del titular de los datos que le concierne frente a injerencias o conductas indebidas ajenas, sin que en ello pueda considerarse un derecho patrimonial de sus datos personales, sino el respeto al derecho fundamental a la protección de datos de carácter personal de los ciudadanos que puede ejercitarse frente a cualquier sujeto público o privado, pero en la presente solo hacemos referencias a los de carácter público.

Así mismo, la presente iniciativa pretende prevenir las violaciones de la privacidad que pudieran resultar del mal tratamiento de las bases de datos, que se encuentran en posesión de los sujetos obligados.

Para finalizar, se debe contemplar que todos los sujetos obligados que tratan datos de carácter personal tienen, correlativa y necesariamente pues, que cumplir deberes jurídicos que permitan hacer efectivo a los titulares de datos el poder de control y disposición sobre sus datos personales, como los siguientes: prestar el previo consentimiento para la obtención y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de sus datos y el conocimiento de que tienen derechos para poder accesar, rectificar, cancelar y oponerse al tratamiento de sus datos personales.

Por lo tanto, el derecho a la protección de datos, se rige por principios internacionales referentes a la protección de este derecho que se traducen en obligaciones de hacer o no hacer de las autoridades.

De tal forma, que los sujetos obligados cuando lleven a cabo el tratamiento de los datos de carácter personal, tendrán que respetar el derecho de los titulares, de que sus datos sean tratados de forma confidencial y legalmente, pues como titulares tienen derecho a ejercer un control y un poder de decisión sobre cuándo, dónde, cómo y por quién son tratados. Dicho control lo pueden exigir a través del Ordenamiento Jurídico competente ante la Comisión de Transparencia y Acceso a la Información del Estado (propuesta su modificación a Instituto) como autoridad independiente y garante encargada de su vigilancia y cumplimiento.

Por lo cual, el derecho fundamental a la protección de datos no es únicamente un derecho de la esfera personal y de libertad que exige la abstención

de los poderes públicos, sino que presenta también una vertiente de prestaciones, que es responsabilidad de los sujetos obligados. Estos servicios o actividades que exigen el tratamiento de datos personales por parte de las autoridades públicas deben garantizar que serán respetados los derechos fundamentales de los ciudadanos.

De igual forma, sabemos que los sujetos obligados necesitan determinados datos de los ciudadanos, para poder prestarles de manera eficaz y eficiente servicios constitucionales legalmente garantizados. Por lo cual, la administración necesita información de los ciudadanos para prestarles los servicios que éstos exigen dentro del Estado. Se puede traducir en que los ciudadanos consienten de alguna manera estos tratamientos de datos por los sujetos obligados en la medida en que le exigen al Estado la prestación efectiva o la garantía de unos derechos sociales, pero deberá estar limitado y regulado el tratamiento de los datos a los que precisamente las atribuciones legales les confieran.

De tal manera, que el aumento de los tratamientos de datos personales por parte de las autoridades nos obliga a ser sensibles para evitar que en el desarrollo de su actividad, se produzcan violaciones de los derechos individuales, como lo es la protección del dato. Los derechos fundamentales, son al mismo tiempo, guía y límite a las actividades de los poderes públicos, ya que al informatizarse, tienden a centralizar e integrar los sistemas de información, convirtiéndose en depositarios de una gran cantidad de información personal, lo que puede provocar que los ciudadanos y los grupos sociales vean disminuida su capacidad de control sobre

sus datos personales, de esta forma los ciudadanos tiene la percepción de sentirse permanentemente observados por las autoridades, síndrome del pez rojo (Los modernos sistemas informáticos permiten vigilar y controlar los movimientos, las relaciones y los vínculos del ciudadano, sin que él se percate de que esta bajo observación. Como algunos notables sociólogos han descrito, el ciudadano se ha convertido en un hombre de cristal ante los poderosos medios informáticos. Otros prefieren llamar esta situación del síndrome del pez rojo, pues como los peces de este color en las urnas de cristal, no tienen un rincón donde esconderse para preservar su intimidad); piensan que la información que tienen las autoridades puede suponer un control público indebido en su esfera personal y afectar a sus derechos, cuando lo que en realidad se pretende es protegerlo. Todo esto repercute en el siempre difícil equilibrio entre los derechos de los ciudadanos la actividad de los poderes públicos, que se hace más poderosa a través de las nuevas tecnologías de la información.

En tal virtud, esta iniciativa tiene como finalidad establecer que el derecho de acceso a la información y el derecho a la protección de los datos personales son derechos autónomos e independientes entre los cuales debe prevalecer el equilibrio. El dato personal debe ser un límite al acceso a la información y la difusión de un dato personal debe realizarse cuando quede plenamente justificado el interés público por revelar dicho datos.

En atención a lo anteriormente expuesto, nos permitimos someter a la consideración de esta Soberanía Popular el siguiente proyecto de:

DECRETO

ARTÍCULO ÚNICO. Se crea la Ley de Protección de Datos Personales para el Estado de Nuevo León, para quedar como sigue:

LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL ESTADO DE NUEVO LEÓN.

TÍTULO PRIMERO
DISPOSICIONES COMÚNES PARA LOS SUJETOS OBLIGADOS

CAPÍTULO ÚNICO
DISPOSICIONES GENERALES

Artículo 1.- La presente Ley es reglamentaria del segundo párrafo del artículo 6º, fracciones III y IV, y segundo párrafo del artículo 15 de la Constitución Política del Estado Libre y Soberano de Nuevo León, es de orden público e interés social y regula el derecho fundamental a la protección de los datos personales en posesión de cualquier autoridad, dependencias, unidad administrativa, entidad, órgano u organismo del Estado y Municipios de Nuevo León; y tiene por objeto, establecer los derechos, procedimientos, tratamientos, responsabilidades, obligaciones, excepciones, sanciones, principios y la debida protección de los datos personales en posesión y resguardo de los sujetos obligados.

Artículo 2.- Son finalidades de la presente Ley:

I. Garantizar la observancia de los principios de protección de datos personales en posesión de los sujetos obligados a que se refiere este ordenamiento;

II. Como el respeto al ejercicio de los derechos de acceso, rectificación, cancelación y oposición del titular del dato;

III. Proveer lo necesario para que toda persona pueda ejercer los derechos de acceso, rectificación y cancelación de sus datos personales, así como manifestar su oposición a determinado tratamiento, mediante procedimientos sencillos y expeditos;

IV. Regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos, u otros medios similares en soporte manual o automatizado y a toda modalidad de uso posterior de los datos de carácter personal; y

V. Promover la adopción de medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos personales.

Artículo 3.- La interpretación de esta ley se realizará conforme a la Constitución Política de los Estados Unidos Mexicanos, la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano, así como la Constitución Política del Estado Libre y Soberano de Nuevo León y la interpretación que dichos tratados hayan realizado los órganos especializados en la materia.

Artículo 4.- Para los efectos de esta Ley se entiende por:

I. **Aviso de Privacidad**: Documento físico, electrónico o en cualquier otro formato generado por el responsable del sistema de datos personales, que es puesto a disposición de su titular, previo al tratamiento de sus datos personales;

II. **Base 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;

III. **Bloqueo:** La conservación de datos personales una vez cumplida la finalidad para las que fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción de éstas. Durante dicho período, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su supresión, en la base de datos que corresponda;

IV. **Cancelación:** Eliminación total de un sistema de datos o de determinados datos del mismo, previo bloqueo de estos;

V. **Clasificación:** Acto por el cual se determina que la información que posee un sujeto obligado es confidencial;

VI. **Instituto:** Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Nuevo León;

VII. **Datos Personales:** Cualquier información concerniente a una persona física identificada o identificable como, la información numérica, alfabética, fotográfica o imagen, gráfica, acústica o de cualquier información, relativa al origen étnico o racial, las características físicas, morales o emocionales, a la vida afectiva y familiar, domicilio particular, número telefónico particular, cuenta personal de correo electrónico, firma electrónica, patrimonio personal y familiar, ideología, opiniones y afiliación política, creencias, convicciones religiosas o filosóficas, estados de salud físico y mental, las preferencias sexuales, la huella digital, ácido desoxirribonucleico (ADN), imagen, número de seguridad social, y toda aquella que permita la identificación de la misma;

VIII. **Datos Personales Sensibles:** Son aquellos que afectan la esfera más íntima de su Titular, se consideran datos personales sensibles aquellos que puedan revelar aspectos como origen étnico o racial; información de salud física o mental, información genética, datos biométricos, firma electrónica, creencias

religiosas, filosóficas o morales; afiliación sindical; opiniones y afiliación política y preferencia sexual;

IX. **Derechos ARCO**: Son los derechos que tienen las personas al Acceso, Rectificación, Cancelación y Oposición de sus datos personales;

X. **Días:** Días hábiles;

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

XII. **Documentos**: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, convenios, contratos, instructivos, notas, memorandos, estadísticas, o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, sonoro, visual, electrónico, informático u holográfico;

XIII. **Documento de Seguridad:** Instrumento que contiene los procedimientos y medidas de seguridad física, administrativa y técnica para garantizar la confidencialidad, integridad y disponibilidad de los datos contenidos en el sistema de datos personales;

XIV. **Encargado:** El servidor público, persona física o jurídica, facultado y nombrado por el responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales;

XV. **Fuentes de Acceso Público:** Aquellas bases de datos, cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que en su caso, el pago de una contraprestación, tarifa o contribución;

XVI. **Hábeas Data:** Es la acción que concede esta Ley al titular de los datos personales de acceder a los registros en poder de los sujetos obligados, para conocer la información que existe sobre su persona y solicitar la rectificación, cancelación u oposición de los mismos;

XVII. **Información Confidencial:** Aquella que se refiere a la vida privada y a los datos personales;

XVIII. **Ley:** Ley de Protección de Datos Personales para el Estado de Nuevo León;

XIX. **Lineamientos**: Disposiciones emitidas por el Instituto que contienen las políticas, criterios y procedimientos, para garantizar a los titulares la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita o inadecuada;

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

XXI. **Medidas de seguridad administrativas:** Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;

XXII. **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:

a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;

b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones de la organización;

c) Proveer a los equipos que contienen o almacenen datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad, y

d) Garantizar la supresión de datos de forma segura;

XXIII. **Medidas de Seguridad Técnicas:** Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;

b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y

d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales;

XXIII. **Prueba de Daño:** Procedimiento para valorar en forma objetiva, cuantitativa y cualitativa, los intereses en conflicto que permitan razonablemente asegurar que los beneficios sociales al divulgar la información de carácter confidencial tienen una alta probabilidad de beneficiar al interés público al ser difundida;

XXIV. **Responsable:** El servidor público titular de la Unidad Administrativa encomendado de las decisiones sobre el tratamiento físico o automatizado

de datos personales, así como el contenido y finalidad de los sistemas de datos personales;

XXV. **Servidor Público:** Los señalados en el artículo 105 de la Constitución Política del Estado y en la Ley de Responsabilidades de los Servidores Públicos del Estado y Municipios de Nuevo León;

XXVI. **Sistema de Datos Personales:** Todo conjunto organizado de archivos, registros, bases o bancos de datos personales de los sujetos obligados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;

XXVII. **Sujeto Obligado:** Cualquier autoridad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, 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 estatal y municipal;

XXVIII. **Tercero:** Persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento;

XXIX. **Titular o Interesado:** Persona física a quien corresponden los datos personales que sean objeto de tratamiento por los sujetos obligados;

XXX. **Transmisión:** Toda comunicación o cesión de datos personales a una persona distinta del interesado o titular. No se considerará como tal la efectuada por los responsables al encargado de los datos personales;

XXXI. **Transmisor:** Sujeto obligado que posee los datos personales objeto de la transmisión;

XXXII. **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o físicos y aplicadas a datos personales, relacionados con la obtención, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos y proporcione al interesado el acceso, rectificación, cancelación u oposición de sus datos, así como su bloqueo, supresión o destrucción;

XXXIII. **Unidades Administrativas:** Las que de acuerdo con la normatividad de cada uno de los sujetos obligados, posean los sistemas de datos personales de conformidad con las facultades que les correspondan; y

XXXIV. **Usuario del Dato:** Persona pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

Artículo 5.- Son sujetos obligados para los efectos de esta Ley, los siguientes:

I. El Poder Ejecutivo del Estado;

II. Las Administraciones Públicas Estatales y Municipales, incluyendo a los organismos desconcentrados y descentralizados, las empresas de participación estatal y municipal, los fideicomisos estatales y municipales, incluyendo los fideicomisos constituidos por los organismos descentralizados y demás entidades del sector paraestatal;

III. El Poder Legislativo, la Auditoría Superior del Estado y cualquiera de sus Órganos;

IV. El Poder Judicial y el Consejo de la Judicatura del Estado;

V. Los Ayuntamientos;

VI. Los Tribunales Administrativos;

VII. Los Organismos Públicos Autónomos y Constitucionales Autónomos del Estado, incluyendo a las Universidades e Instituciones de Educación Superior Pública.

VIII. Partidos Políticos; y

IX. Sindicatos.

Artículo 6.- En todo lo no previsto por esta Ley, se aplicarán de manera supletoria la Ley de Transparencia y Acceso a la Información del Estado de Nuevo León, la Ley de Justicia Administrativa para el Estado de Nuevo León y el Código de Procedimientos Civiles para el Estado de Nuevo León.

TÍTULO SEGUNDO
DE LOS PRINCIPIOS EN MATERIA DE DATOS PERSONALES

CAPÍTULO PRIMERO
PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Artículo 7.- Toda persona tiene derecho a la protección de su vida privada, sus datos personales y la información relacionada con los mismos, la cual será custodiada, protegida, manejada y en su caso actualizada en los términos de la presente ley.

Los sujetos obligados al tratar los sistemas de datos, deberán cumplir los principios de consentimiento, información previa, finalidad, licitud, calidad de la información, confidencialidad, seguridad, proporcionalidad, máxima privacidad, responsabilidad e irrenunciabilidad, así como garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los titulares de los datos personales o sus legítimos representantes. Adoptando las medidas necesarias para su aplicación. Lo anterior aún y cuando estos datos sean tratados por un tercero a solicitud del sujeto obligado.

El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al Titular del dato, será respetado en todo momento por él o por los terceros a los que les solicite el tratamiento de los datos.

Artículo 8.- El Principio de Calidad de la Información es en el cual, el sujeto obligado dará tratamiento a los datos personales cuidando que estos sean ciertos, adecuados, pertinentes y no excesivos en relación con el ámbito y la finalidad para los que se hubieren obtenido.

Artículo 9.- El Principio de Confidencialidad consiste en garantizar que exclusivamente las personas autorizadas para su tratamiento en términos de la Ley, además del propio titular del dato, podrán acceder a los datos personales que obren en poder del sujeto obligado.

No podrá invocarse el carácter confidencial cuando se trate de investigaciones relacionadas con violaciones graves de derechos fundamentales o delitos de lesa humanidad.

Dicha obligación subsistirá aun después de finalizada la relación entre el sujeto obligado con el titular de los datos personales, así como después de finalizada la relación laboral entre el sujeto obligado y el responsable del sistema de datos personales o los usuarios.

Artículo 10.- El Principio de Consentimiento es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el titular o interesado consienta el tratamiento de datos personales que le concierne.

Los sujetos obligados no podrán difundir o transmitir los datos personales contenidos en los sistemas de datos desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso de los interesados a que haga referencia la información. Al efecto el sujeto obligado contará con los formatos necesarios para recabar dicho consentimiento, pudiendo utilizarse en su caso medios electrónicos.

El consentimiento del titular para el tratamiento de sus datos personales, deberá ser expreso de acuerdo con la naturaleza del tratamiento, cuando así lo requiera una ley o los datos sean tratados para finalidades distintas.

Artículo 11.- No será necesario el consentimiento del titular o interesado para la obtención de los datos personales cuando:

I. Se recaben para el ejercicio de las atribuciones legales conferidas a los sujetos obligados;

II. Se refieran a las partes de un contrato o precontrato de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

III. Sean necesarios para efectuar un tratamiento para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente;

IV. Se trate de datos obtenidos de fuentes de acceso público y se requiera su tratamiento; y

V. Tengan por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Artículo 12.- El Principio de Finalidad consiste en que los sujetos obligados solo deberán utilizar los datos personales para el fin u objetivo para el cual fueron recabados y tratados los mismos.

Artículo 13.- El Principio de Máxima Privacidad es el principio rector de la protección del dato personal, por el cual los sujetos obligados tendrán como

principal prioridad, proteger y resguardar la intimidad y privacidad de los datos personales, que se encuentran bajo su resguardo.

Artículo 14.- El Principio de Información Previa consiste en dar a conocer al interesado o titular, la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales, el cual se cumple a través de los avisos de privacidad, de conformidad con lo previsto en la presente ley.

Artículo 15.- El Principio de Irrenunciabilidad es en el que los datos personales son irrenunciables e intransferibles, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular o de su representante legal.

Artículo 16.- El Principio de Licitud consiste en que el tratamiento de datos personales debe realizarse únicamente por los sujetos obligados que cuenten con atribuciones legales, reglamentarias o normativas para tal efecto, debiendo obtener los datos a través de los medios previstos en dichas disposiciones.

Artículo 17.- El Principio de Proporcionalidad establece que sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.

Artículo 18.- El Principio de Responsabilidad consiste en que el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquellos que haya comunicado a un encargado o tercero legalmente autorizado; valiéndose para ello de los estándares señalados en la presente Ley y los que se establezcan en el documento de seguridad por el sujeto obligado competente.

Artículo 19.- El Principio de Seguridad es el deber de todo responsable y encargados de llevar a cabo el tratamiento de datos personales manteniendo y garantizando las medidas de seguridad administrativas, técnicas y físicas establecidas en el documento de seguridad, que permitan proteger los datos

personales contra daño, pérdida, alteración, destrucción o bien, el uso, acceso o tratamiento no autorizado.

CAPÍTULO SEGUNDO
AVISO DE PRIVACIDAD

Artículo 20.- El aviso de privacidad se pondrá a disposición de los titulares o del interesado a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se obtiene el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y

II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, la identidad y domicilio del responsable que los recaba, las finalidades de tratamiento de datos, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Artículo 21.- El sujeto obligado tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y su finalidad, a través del aviso de privacidad.

Los requisitos que debe contemplar como mínimo el aviso de privacidad son:

I. Identidad del sujeto obligado;

II. Indicación respectiva que señale que los datos serán incorporados a un sistema de base de datos;

III. La finalidad del tratamiento de los datos que proporcione el titular del dato;

IV. Los destinatarios de los datos personales proporcionados;

V. Del carácter obligatorio o facultativo de la entrega de los datos personales;

VI. De las consecuencias de la negativa a no suministrarlos;

VII. De las transmisiones o posibilidad de transmisión de los datos proporcionados, en cuyo caso deberá constar el consentimiento expreso de la persona, salvo las excepciones que marque la Ley;

VIII. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición;

IX. Del cargo y dirección del responsable de la base de datos; y

X. Fecha de la última actualización del aviso de privacidad.

Cuando se utilicen cuestionarios u otros impresos o medios electrónicos para la obtención, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el presente Artículo.

Cuando los datos personales no hayan sido obtenidos del interesado, el responsable del sistema de datos personales deberá dar a conocer el aviso de privacidad, a través de mecanismos impresos, sonoros, visuales, electrónicos o cualquier otro, dentro de los tres meses siguientes al momento del registro de los datos, salvo que existan constancia de que el interesado ya fue informado del contenido de las fracciones II, III, IV, VII, VIII y IX.

TÍTULO TERCERO
DE LOS DERECHOS EN MATERIA DE DATOS PERSONALES

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

Artículo 22.- Los derechos de acceso, rectificación, cancelación y oposición de datos personales son derechos independientes, de tal forma que no puede

entenderse que el ejercicio de alguno de ellos sea requisito previo o impida el ejercicio de otro. La procedencia de estos derechos, en su caso, se hará efectiva una vez que el titular del dato o su representante legal acrediten su identidad o representación, respectivamente.

Artículo 23.- El titular o interesado, en los términos previstos en esta Ley, tiene derecho a acceder, solicitar y ser informado gratuitamente sobre sus datos personales que estén en posesión del sujeto obligado, el origen de dichos datos, el tratamiento del cual sean objeto, las transmisiones realizadas o que se pretendan realizar, así como a tener acceso al aviso de privacidad al que está sujeto el tratamiento, en los términos previstos en esta ley.

El responsable del tratamiento, debe responder al ejercicio del derecho de acceso, tenga o no datos de carácter personal del interesado en su sistema de datos.

Artículo 24.- El titular o interesado tendrá derecho a solicitar la rectificación de sus datos personales cuando sean inexactos, incompletos, siempre que sea posible y no exija esfuerzos desproporcionados, a criterio de la autoridad competente en la materia.

En términos de los lineamientos emitidos por la Comisión, quien decidirá en definitiva, cuando la rectificación resulte imposible o exija esfuerzos desproporcionados.

La rectificación podrá hacerse de oficio, cuando el responsable del tratamiento tenga en su posesión los documentos que acrediten la inexactitud de los datos.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la rectificación o cancelación, el responsable del tratamiento deberá notificarlo dentro de los treinta días siguientes a quien se hayan transmitido, quien deberá a su vez realizar la rectificación o cancelación correspondiente.

Artículo 25.- El titular del dato tendrá derecho a solicitar la cancelación de sus datos personales cuando:

I. El tratamiento de los mismos no se ajuste a lo dispuesto por la Ley, sus reglamentos o los lineamientos respectivos;

II. Hubiere ejercido el derecho de oposición y este haya resultado procedente; y

III. Los datos personales hayan dejado de ser necesarios para el cumplimiento de la finalidad de la base de datos, de conformidad con las disposiciones aplicables o en el aviso de privacidad y para los cuales hayan sido requeridos.

Artículo 26.- La cancelación dará lugar al bloqueo del dato por un periodo de tres meses en el que el responsable lo conservará precautoriamente para efectos de responsabilidades nacidas del tratamiento.
Cumplido el periodo a que se refiere el párrafo anterior, deberá procederse a la cancelación del dato, que implica el borrado o eliminación del mismo de la base de datos.
La cancelación procederá de oficio cuando el responsable de la base de datos, estime que dichos datos resultan inadecuados o excesivos o cuando haya concluido la finalidad para la cual fueron recabados.

Articulo 27.- El responsable no estará obligado a cancelar los datos personales cuando:

I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;

II. Deban ser tratados por disposición legal;

III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, de investigación y persecución de delitos o la actualización de sanciones administrativas;

IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;

V. Sean necesarios para realizar una acción en función del interés público;

VI. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Artículo 28.- El titular o interesado tendrá derecho a oponerse al tratamiento de sus datos personales, en el supuesto que estos se hubieren recabado sin su consentimiento, cuando existan motivos fundados para ello y la Ley no disponga lo contrario. De actualizarse tal supuesto, el responsable deberá excluir del tratamiento los datos relativos al interesado.
La procedencia del derecho de oposición, dará lugar a la cancelación del dato, previo bloqueo del mismo.

Artículo 29.- Cualquier persona podrá iniciar ante el Instituto un procedimiento para denunciar violaciones a las disposiciones contenidas en la presente Ley. En este caso, el Instituto procederá a revisar la denuncia para que, de considerarla procedente, en un plazo no mayor a 15 días hábiles emita una resolución en la que ordene al sujeto obligado las medidas que considere necesarias para remediar la violación en el menor tiempo posible, previa audiencia del sujeto obligado.

Cuando el Instituto tenga conocimiento, por cualquier otro medio, de posibles violaciones a las disposiciones de la Ley o los lineamientos, podrá iniciar de oficio la investigación respectiva.

Cuando derivado de la investigación de los casos de violación del derecho a la protección de datos personales, se desprenda que puede existir menoscabo de otros derechos humanos correlativos, el Instituto se coordinara con las instancias u organismos competentes, para la investigación correspondiente, con la finalidad de garantizar cabalmente la protección integral de dichos derechos humanos.

CAPÍTULO SEGUNDO
DEL PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

Articulo 30.- Sin perjuicio de lo que dispongan otras Leyes, sólo los titulares o sus representantes legales podrán solicitar al sujeto obligado correspondiente, que les de acceso, rectifique, cancele o haga efectivo su derecho de oposición, respecto de

los datos personales que le conciernan y que obren en un sistema de datos personales en posesión de los sujetos obligados.

Artículo 31.- La solicitud de derechos de acceso, rectificación, cancelación y oposición deberá contener:

I. El nombre del solicitante y domicilio para recibir notificaciones, mismo que deberá estar ubicado en el lugar donde resida la unidad de acceso ante la que se presente la solicitud;

II. Descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos antes mencionados;

III. Cualquier otro elemento o documento que faciliten la localización de los datos personales;

IV. Opcionalmente la modalidad en la que se prefiere se otorgue el acceso a sus datos personales, la cual podrá ser mediante consulta directa, copias simples, certificadas o cualquier otro medio; y

V. Documentos que acrediten la personalidad del titular o de su representante legal.

Al solicitarse la rectificación o cancelación de datos personales, se deberá anexar la documentación original que acredite la veracidad de lo solicitado, cuando la naturaleza del dato personal permita contar con tal documentación e indicar las modificaciones a realizarse.

Artículo 32.- La solicitud de acceso, rectificación, cancelación o de oposición de datos personales podrá formularse verbalmente, mediante escrito libre, a través de los formatos que deberá proporcionar el sujeto obligado o por medios electrónicos, en este último caso se podrá establecer un correo electrónico donde se recibirán las solicitudes o crearse un sistema para este propósito.

Tratándose de solicitudes de acceso, rectificación, cancelación o de oposición de datos personales, así como del procedimiento de inconformidad que sean

realizadas por medios electrónicos, los sujetos obligados, excepto los municipios con población inferior a setenta mil habitantes, deberán crear un sistema electrónico para efecto de su recepción, trámite y seguimiento, cuyo procedimiento deberá ser publicado en términos claros en su página oficial de internet y contando con los debidos elementos de seguridad.

Las solicitudes presentadas de manera electrónica se tendrán por recibidas en la fecha asentada en el registro electrónico del equipo receptor de la misma.

El procedimiento de acceso, rectificación, cancelación u oposición de datos personales, iniciará con la presentación de una solicitud en cualquiera de las siguientes modalidades:

I. Por escrito material, será la presentada personalmente por el titular del dato o su representante legal, en la oficina de información pública, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;

II. En forma verbal, será la que realiza el titular del dato o su representante legal directamente en la oficina de información pública, de manera oral y directa, la cual deberá ser capturada por el responsable de la oficina en el formato respectivo;

III. Por correo electrónico, será la que realiza el titular del dato o su representante legal a través de una dirección electrónica y será enviada a la dirección de correo electrónico asignada a la oficina de información pública del sujeto obligado;

IV. Por el sistema electrónico que el Instituto establezca para tal efecto; y

V. Cuando se refiera a el derecho de acceso, se podrá presentar la solicitud por correo, pero la información se entregara en el domicilio del sujeto obligado, previa la acreditación de la identidad del titular del dato.

Así mismo, en relación al ejercicio del derecho de cancelación, la solicitud deberá indicar si revoca el consentimiento otorgado.

Si se niega al titular, total o parcialmente el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, o a falta de respuesta a su solicitud dentro del término legal, éste podrá interponer el procedimiento de inconformidad previsto en el Título Noveno de la presente Ley.

Artículo 33.- Los sujetos obligados deberán orientar en forma sencilla y comprensible a toda persona sobre los tramites y procedimientos que deben efectuarse para ejercer sus derechos de acceso, rectificación, cancelación y oposición de sus datos personales, las autoridades o instancias competentes, la forma de realizarlos, la manera de llenar los formularios que se requieran, así como las instancias ante las que se puede acudir a solicitar orientación o formular quejas, consultas o reclamos sobre la presentación del servicio o sobre el ejercicio de las funciones o competencias a cargo de los servidores públicos de que se trate.

Artículo 34.- Los medios por los cuales el solicitante podrá recibir notificaciones o acuerdos serán: correo electrónico, a través del sistema electrónico instrumentado por el sujeto obligado y por el Instituto, o notificación personal en su domicilio o en la propia Unidad de información que corresponda, cuando se encuentre dentro del mismo. En el caso de que el solicitante no señale domicilio o algún medio para oír y recibir notificaciones, el acuerdo o notificación se dará a conocer por lista que se fije en los estrados del sujeto obligado que corresponda.

Artículo 35.- Si los datos proporcionados por el solicitante no bastan para la localización de la información, son imprecisos o erróneos, el sujeto obligado prevendrá al solicitante en un plazo no mayor de diez días, contados a partir de la recepción de la solicitud, para que en un término de cinco días, la complemente o aclare.

En caso de no cumplir con dicha prevención o la misma fuera extemporánea, se tendrá por no presentada la solicitud.

Artículo 36.- La respuesta a una solicitud deberá ser notificada al titular en el menor tiempo posible, que no podrá exceder de diez días hábiles, contados a partir del día siguiente de la presentación de aquélla. Además, se precisará el costo de reproducción, si lo hubiere y la modalidad en que será entregada la información, atendiendo en la mayor medida de lo posible a la solicitud del titular.

Este plazo podrá prorrogarse por un periodo igual cuando no sea posible dar respuesta en dicho término. El sujeto obligado deberá comunicar al solicitante, antes del vencimiento del plazo, la justificación y razones válidas por las cuales hará uso de la prórroga. No podrán invocarse como causales de ampliación del plazo motivos que supongan negligencia o descuido del sujeto obligado en el desahogo de la solicitud.

Artículo 37.- Si se niega al interesado, total o parcialmente el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, o a falta de respuesta a su solicitud dentro del término legal de diez días hábiles, éste podrá interponer el recurso de revisión previsto en el Título Noveno de la presente Ley.

Artículo 38.- Salvo los costos de reproducción de la información previstos en los ordenamientos correspondientes, el acceso a los datos personales será gratuito, la entrega correspondiente se realizará al solicitante de manera personal y en el domicilio del sujeto obligado.

TÍTULO CUARTO
TRATAMIENTO Y REGISTRO DE DATOS PERSONALES

CAPÍTULO PRIMERO
SISTEMAS Y TRATAMIENTOS DE DATOS PERSONALES

Artículo 39.- Los Sistemas de Datos Personales, ya sean físicos o automatizados deben ser protegidos contra riesgos de pérdida o de acceso, destrucción, uso, modificación o divulgación no autorizados.

Artículo 40.- La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:

I. Cada sujeto obligado deberá publicar en el Periódico Oficial del Estado la creación, modificación o supresión de los sistemas de datos personales que tengan en su posesión.

II. Cada sujeto obligado deberá informar al Instituto sobre la creación, modificación o supresión de su sistema de datos personales;

III. En caso de creación o modificación de sistemas de datos personales, se deberán incluir en el Registro, los datos previstos en el siguiente artículo;

IV. En las disposiciones que se dicten para la supresión de los sistemas de datos personales, se establecerá el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción; y

V. De la destrucción de los datos personales podrán ser excluidos aquellos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.

En el caso de que el tratamiento de los sistemas haya sido realizado por persona física o moral, distinta al sujeto obligado, el instrumento jurídico que dio origen al mismo deberá establecer el plazo de conservación por el usuario, al término del cual los datos deberán ser devueltos en su totalidad al sujeto obligado, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

Artículo 41.- Los sujetos obligados deberán registrar ante el Instituto los Sistemas de Datos Personales que posean. El registro deberá indicar por lo menos los siguientes datos:

I. El Sujeto obligado que tiene a su cargo la base de datos;

II. La denominación de la base de datos y el tipo de datos personales objeto de tratamiento;

III. El nombre y cargo del responsable y los usuarios;

IV. La normatividad aplicable que de fundamento al tratamiento;

V. La finalidad del tratamiento;

VI. La forma de recolección y actualización de datos;

VII. El destino de los datos y personas físicas o jurídicas colectivas a las que pueden ser transmitidos;

VIII. El modo de interrelacionar la información registrada;

IX. La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición;

X. El tiempo de conservación de los datos; y

XI. Las medidas de seguridad.

Artículo 42.- Quedan prohibidos los sistemas de datos personales creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen ideología política o filosófica, afiliación sindical, religión, creencias, origen racial o étnico, preferencia sexual, características morales o emocionales o convicciones religiosas. Por lo cual, ninguna persona está obligada a proporcionar datos personales considerados sensibles o de nivel alto.

No obstante lo dispuesto en el apartado anterior, podrán ser objeto de tratamiento los datos personales cuando resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando medien razones de interés general, así lo disponga una ley, consienta expresamente el titular del dato o interesado mediante firma autógrafa, sea necesario para salvaguardar la vida o integridad física del titular o interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, tengan fines estadísticos, históricos o cuando se hubiere realizado previamente el procedimiento de disociación.

Tratándose de estudios científicos o de salud pública el procedimiento de disociación no será necesario.

CAPÍTULO SEGUNDO
DE LA VIDEO VIGILANCIA

Artículo 43.- La video vigilancia comprende cualquier grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Las referencias contenidas en este capítulo a videocámaras y cámaras se entenderán hechas también por cualquier medio técnico análogo y, en general a cualquier sistema que permita los tratamientos previstos en la misma.

Artículo 44.- No se considerará base de datos al tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Artículo 45.- Los sujetos obligados deberán:

a) Colocar en las zonas video vigiladas al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados; y

b) Tener a disposición de los interesados, impresos en los que se detalle la información prevista por el artículo 21 de la presente ley, en cumplimento del principio de información previa.

Los sujetos obligados tratarán las imágenes cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explicitas, que hayan justificado la instalación de las cámaras o video cámaras.

Artículo 46.- Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

Los Sujetos Obligados que cuenten con sistemas de video vigilancia deberán cumplir con el deber de información previsto en el artículo 21 de la presente Ley.

Artículo 47.- Para el ejercicio de los derechos de acceso y cancelación de protección de datos de carácter personal, el afectado deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada.

El responsable deberá facilitar el derecho de acceso mediante escrito en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la presente Ley.

Artículo 48.- El interesado al que se deniegue total o parcialmente el ejercicio de los derechos, podrá reclamar su tutela mediante el recurso de revisión ante el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado.

Artículo 49.- Los datos serán cancelados en el plazo máximo de un mes desde su captación.

Artículo 50.- El sujeto obligado que prevea la creación de bases de datos de video vigilancia deberá notificarlo al Instituto, para agregarlo en el Registro de listados de bases de datos.

Artículo 51.- El responsable deberá adoptar las medidas de índole técnica y organizativas y administrativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Artículo 52.- Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos de carácter personal deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El Sujeto obligado deberá informar a las personas con acceso a los datos del deber de secreto.

Artículo 53.- El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por Seguridad Pública se regirá por las disposiciones sobre la materia.

Sin perjuicio de lo establecido en este capítulo, la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.

Artículo 54.- Deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

CAPÍTULO TERCERO
BOLETINES JUDICIALES, LISTAS DE ACUERDOS Y ESTRADOS

Artículo 55.- Tratándose de la debida protección de datos personales contenidos en las sentencias, resoluciones, actuaciones o notificaciones en materia judicial, electoral o administrativa del Estado, esta se sujetará a lo dispuesto por los respectivos reglamentos o acuerdos generales que al efecto deberán expedir cada autoridad, cuidando en todo momento, no disminuir o contradecir los principios y garantías contenidos en la presente Ley, debiendo tener especial cuidado en la protección de los datos personales sensibles y los relacionados con menores o adolecentes.

Artículo 56.- En los casos en que sea estrictamente necesario realizar notificaciones con publicación de datos personales, mediante medios informáticos, digitales o de internet, una vez efectuada aquélla y transcurridos los plazos de ejercicio de los posibles recursos, no se mantendrán dichos datos para su localización a través de los buscadores electrónicos. Al efecto, se establecerán las indicaciones oportunas para limitar la indexación del nombre y apellidos de las personas en los mencionados documentos mediante la utilización de la respectiva tecnología informática, con objeto de que los motores de búsqueda de internet no puedan asociarlo al titular.

TÍTULO QUINTO
TRANSMISIÓN DE LOS DATOS PERSONALES

CAPÍTULO ÚNICO
TRANSMISIÓN DE LOS DATOS PERSONALES

Artículo 57.- El responsable deberá garantizar el manejo confidencial de los datos personales, por lo que no podrán divulgarse o transmitirse salvo por disposición legal o cuando medie el consentimiento expreso del titular del dato mediante la firma autógrafa o bien, a través de un medio de autentificación similar.

Los responsables sólo podrán transmitir los sistemas de datos personales a terceros particulares siempre y cuando se estipule, en el contrato respectivo, la obligación del tercero de aplicar las medidas de seguridad y custodia previstas en el presente título, así como la imposición de penas convencionales por su incumplimiento.

Lo anterior, sin perjuicio de las responsabilidades civiles o penales a que hubiere lugar, por el uso inadecuado o la utilización distinta a la finalidad para la cual fueron recabados los datos contenidos en los sistemas de datos personales.

El servidor público encargado de recabar el consentimiento del titular, deberá informar previamente a este, la identidad del destinatario, el fundamento que autoriza la transmisión, la finalidad de la transmisión y los datos personales a transmitir, así como las implicaciones de otorgar, de ser el caso, su consentimiento.

Artículo 58.- Los sujetos obligados podrán realizar la transmisión de datos cuando se cumplan las siguientes condiciones:

I. Que haya mediado el consentimiento expreso del titular;

II. Que el uso que se les vaya a dar mantenga congruencia con la finalidad para la cual se obtuvieron; y

III. Que se celebre contrato de transferencia, el cual deberá contener como mínimo:

a) La designación y obligación del responsable y de los encargados, de guardar la debida confidencialidad de los datos personales contenidos en el sistema de datos personales;

b) La posibilidad de incurrir en las responsabilidades y sanciones civiles o penales que correspondan por el uso inadecuado de los datos;

c) El nivel o niveles de protección requeridos para los datos de acuerdo con su naturaleza; y

d) La obligación de permitir verificaciones a las medidas de seguridad adoptadas mediante la inspección de la información y documentación que se estimen necesarias.

Artículo 59.- El consentimiento para la transmisión de los datos de carácter personal es revocable, mediante aviso o escrito que realice ante el sujeto obligado.

Artículo 60.- No se requerirá el consentimiento previo del interesado para la transmisión de sus datos entre sujetos obligados en los siguientes supuestos:

I. Cuando esté previsto en una Ley;

II. Cuando se trate de datos obtenidos de fuentes de acceso público;

III. Cuando la transmisión se realice al Ministerio Público en el ejercicio de sus atribuciones oficiales de investigación y persecución de los delitos, así como a los órganos jurisdiccionales en el ejercicio de sus funciones;

IV. Se trate de datos obtenidos por los sujetos obligados en el ámbito de su competencia y sean utilizados para el mismo objeto; y

V. Tengan por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Artículo 61.- Los datos de carácter personal recabados o elaborados por los sujetos obligados para el desempeño de sus atribuciones, podrán ser transmitidos a otros sujetos obligados, siempre que exista fundamento legal para ello, y sea necesario para el ejercicio de competencias que versen sobre la misma materia.

En caso de que los destinatarios sean instituciones de otras entidades federativas, se deberá asegurar que tales instituciones garanticen que cuentan con niveles de protección, semejantes o superiores, a los establecidos en esta ley y, en la propia normatividad del sujeto obligado de que se trate.

Si se trata personas o instituciones de otros países, el responsable del sistema de datos personales deberá realizar la cesión de los mismos, conforme a las disposiciones previstas en la legislación federal aplicable, siempre y cuando se garanticen los niveles de seguridad y protección previstos en la presente ley.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente, respondiendo solidariamente por la inobservancia de las mismas.

Artículo 62.- No se considerarán transmisiones, las efectuadas entre el responsable y el encargado de los datos personales y las realizadas entre Unidades Administrativas adscritas al mismo sujeto obligado en el ejercicio de sus atribuciones.

Artículo 63.- Los sistemas de datos personales creados para fines administrativos por las autoridades de seguridad pública, estarán sujetos al régimen general de la presente Ley y en la Ley de Seguridad Pública para el Estado de Nuevo León.

La obtención y tratamiento de los datos sensibles por las autoridades de seguridad pública podrá realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas, en su caso, por los titulares de los datos que corresponden ante los órganos jurisdiccionales.

Artículo 64.- La obtención y tratamiento de datos de carácter personal por parte de las autoridades a cargo de la seguridad pública, sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten legalmente necesarios, de conformidad con los ordenamientos aplicables.

Artículo 65.- Los responsables de los sistemas que contengan los datos a que se refiere el artículo anterior podrán negar el acceso, la rectificación, la cancelación u oposición en función del daño probable que pudieran derivarse para la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

La aplicación de estas reglas en materia de seguridad pública seguirán los principios generales junto con la legislación específica de la materia, sin que las leyes puedan suprimir el derecho de acceso, rectificación, cancelación u oposición de modo permanente.

Artículo 66.- Los sujetos obligados que posean sistemas de datos en materia tributaria, consideren prudente negar el ejercicio de los derechos de protección de datos personales, deberán elaborar y detallar mediante acuerdo debidamente fundado y motivado en la presente Ley, las causales que consideran obstaculizan el debido cumplimiento de sus obligaciones y actividades administrativas en materia fiscal, el cual, podrá ser impugnado ante el Instituto.

TÍTULO SEXTO
DE LA SEGURIDAD DE LOS DATOS PERSONALES

CAPÍTULO PRIMERO
MEDIDAS DE SEGURIDAD

Artículo 67.- Los sujetos obligados deberán elaborar un documento en el que se establezca las medidas adoptadas para proteger los sistemas o archivos de información contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos, la contaminación por virus informáticos u otras causas de naturaleza similar a las enunciadas, de acuerdo al tipo y nivel de datos contenidos en dichos sistemas y con base en los estándares internacionales de seguridad.

Artículo 68.- El sujeto obligado responsable de la protección y tratamiento del sistema de datos personales, adoptará las medidas de seguridad, conforme a los tipos de seguridad:

I. **Física.-** Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor;

II. **Lógica.-** Se refiere a las medidas de protección que permiten la identificación y autentificación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función;

III. **De Desarrollo y Aplicaciones.-** Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas;

IV. **De Cifrado.-** Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integridad y confidencialidad de la información; y

V. **De Comunicaciones y Redes.-** Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

Artículo 69.- Las medidas de seguridad deberán establecerse atendiendo a la siguiente clasificación:

Sección I: Nivel básico.

Los sistemas de datos personales que contienen alguno de los datos que se enuncian a continuación deberán aplicar las medidas de seguridad de nivel básico. Este nivel de seguridad es aplicable a todos los sistemas de datos personales:

De Identificación: Nombre, domicilio, número de teléfono particular, número de teléfono celular, dirección de correo electrónico, estado civil, firma, firma electrónica, Registro Federal de Contribuyentes, Clave Única de Registro de Población, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad,

nombres de familiares dependientes y beneficiarios, imagen, idioma o lengua, entre otros.

Laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Dichas medidas, de nivel básico, corresponden a los siguientes aspectos:

a) Documento de seguridad. Es un documento de carácter interno que debe reflejar por escrito todo lo relacionado con las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar la seguridad de los datos. Dicho documento debe ser elaborado por el responsable del sistema de datos y, en su caso, por el encargado del tratamiento, y es obligatorio para todo el personal que tenga acceso a los sistemas de información;

b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales. El titular u órgano de dirección del sujeto obligado, en coordinación con el responsable del Sistema de Datos Personales, adoptarán las medidas necesarias para que los servidores públicos del sujeto obligado conozcan las normas de seguridad y las responsabilidades y consecuencias en que se pudiera incurrir en caso de incumplimiento;

c) Registro de incidencias. Para tal efecto se hará constar el momento y el tipo de incidencia ocurrida y se establecerán los procedimientos de notificación, gestión y respuesta;

d) Identificación y autentificación. Consistente en la obligación del responsable de adoptar medidas para que los encargados y usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. Para tal efecto, el responsable deberá mantener

actualizada una relación de personas autorizadas y los accesos autorizados para cada una de ellas;

e) Control de acceso, que implica que el responsable deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo por las personas autorizadas en el sistema de datos personales, así como la facultad del responsable de conceder, alterar o anular la autorización para el acceso a los sistemas de datos personales;

f) Gestión de soportes. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento quedando constancia motivada de ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o ajenos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

La identificación de soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles, se podrá realizar

utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos, identificar su contenido, y que dificulten la identificación para el resto de personas; y

g) Copias de respaldo y recuperación. Esto es, que en caso de que los datos personales se encuentren en soporte físico, se procurará que el respaldo se efectúe mediante la digitalización de los documentos, mientras que para soportes electrónicos se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la perdida involuntaria o destrucción accidental.

El responsable se encargará de verificar, al menos, cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Sección II. Nivel medio.

Los sistemas de datos personales que contengan alguno de los datos que se enuncian a continuación, además de cumplir con las medidas de seguridad de nivel básico, deberán observar las identificadas con nivel medio.

Datos Patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

Datos sobre procedimientos jurisdiccionales o administrativos seguidos en forma de juicio: Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Datos Académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

Tránsito y movimientos migratorios: Información relativa al movimiento de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Este nivel, deberá considerar los siguientes aspectos, adicionalmente de las del nivel básico:

a) Responsable de seguridad. El sujeto obligado designará uno o varios responsables de seguridad para coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación podrá ser única para todos los sistemas de datos en posesión del sujeto obligado, o diferenciada, dependiendo de los métodos de organización y tratamiento de los mismos. En todo caso dicha circunstancia deberá especificarse en el documento de seguridad;

En ningún caso esta designación supone una delegación de las facultades y atribuciones que corresponden al responsable del sistema de datos personales;

b) Auditoría. Las medidas de seguridad implementadas para la protección de los sistemas de datos personales se someterán a una auditoría interna o externa, mediante la que se verifique el cumplimiento de las disposiciones de esta Ley y demás procedimientos vigentes en materia de seguridad de datos, al menos, cada dos años;

El informe de resultados de la auditoría deberá dictaminar sobre la adecuación de las medidas de seguridad previstas en esta ley, así como en las recomendaciones instrucciones, lineamientos, criterios, que en su caso, haya emitido el Instituto. Además, deberá identificar sus deficiencias y proponer las medidas preventivas, correctivas o complementarias necesarias.

El informe de auditoría así como las medidas correctivas derivadas de la auditoría deberá ser comunicado por el responsable al Instituto dentro de los veinte días siguientes a su emisión u observancia;

c) Control de acceso físico. El acceso a las instalaciones donde se encuentren los sistemas de datos personales, ya sea en soporte físico o electrónico, deberá permitirse exclusivamente a quienes estén expresamente autorizados en el documento de seguridad; y

d) Pruebas con datos reales. Las pruebas que se lleven a cabo con efecto de verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación o modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados. Si se realizan pruebas con datos reales, se elaborará con anterioridad una copia de respaldo.

Sección III: Nivel alto.

Los sistemas de datos personales que contengan alguno de los datos que se enuncian a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las identificadas con nivel alto.

Datos Ideológicos y religiosos: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.

Datos de Salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.

Características personales: Tipo de sangre, ADN, huella digital, u otros análogos.

Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.
Origen: Étnico y racial.

Los niveles de seguridad alto deberán incorporar las medidas de los niveles anteriores, además de las siguientes:

a) **Distribución de soportes.** La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión;

b) **Registro de acceso.** El acceso a los sistemas de datos se limitará exclusivamente al personal autorizado, estableciendo mecanismos que permitan identificar los accesos realizados en el caso en que los sistemas puedan ser utilizados por múltiples autorizados. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad correspondiente, sin que se permita la desactivación o manipulación de los mismos.

   De cada acceso se guardarán, al menos, la identificación del usuario, la fecha y hora en que se realizó, el sistema accedido, el tipo de acceso y si este fue autorizado o denegado.

   El periodo de conservación de los datos consignados en el registro de acceso será de, al menos, dos años; y

c) **Telecomunicaciones.** La transmisión de datos de carácter personal, a través de redes públicas o redes inalámbricas de comunicaciones electrónicas, se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

Las medidas de seguridad constituyen los mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales.

CAPÍTULO SEGUNDO
DE LAS OBLIGACIONES DEL RESPONSABLE

Artículo 70.- Los titulares de los sujetos obligados designarán al responsable y encargado de los sistemas de datos personales, para el cumplimiento de la presente Ley, sin que ello implique eximir de responsabilidades a los sujetos obligados por el incumplimiento de este ordenamiento.

Los responsables, en el tratamiento de datos personales, tendrán las siguientes obligaciones:

I. Asegurar la protección de los datos personales en su posesión;

II. Permitir el acceso de los particulares a sus datos personales, y en su caso ejercer los derechos de rectificación, cancelación u oposición;

III. Cumplir con las políticas y lineamientos así como las normas aplicables para el manejo, tratamiento, seguridad y protección de datos personales;

IV. Adoptar el nivel de las medidas de seguridad necesarias para la protección de datos personales y comunicarlas al Instituto para su registro, en los términos previstos en esta Ley;

V. Elabora y presentar al Instituto un informe correspondiente sobre las obligaciones previstas en la presente Ley, a más tardar el último día del mes de enero de cada año. La omisión de dicho informe será motivo de responsabilidad;

VI. Contar con el consentimiento del titular para la obtención de sus datos personales, informándole previamente sobre la existencia y finalidad del archivo o sistema de datos, así como el carácter obligatorio u optativo de proporcionarlos y las consecuencias de ello;

VII. Adoptar los procedimientos adecuados para dar trámite a las solicitudes de acceso, rectificación, cancelación y oposición de datos personales, y en su caso, para la cesión de los mismos, debiendo capacitar a los servidores públicos encargados de su atención y seguimiento;

VIII. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;

IX. Proceder a la cancelación de los datos personales cuando éstos dejen de ser necesarios para la finalidad para la cual se obtuvieron. No se considerará como finalidad distinta, el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que no puedan atribuirse a persona determinada o determinable, así como para fines históricos;

X. Actualizar los datos personales cuando haya lugar, debiendo corregir o completar de oficio aquellos que fueren inexactos o incompletos, respectivamente, a efecto de que coincidan con los datos presentes del titular del dato, siempre y cuando se cuente con el documento que avale la actualización de dichos datos. Lo anterior, sin perjuicio del derecho del titular del dato para solicitar la rectificación o cancelación de los datos personales que le conciernen;

XI. Elaborar el documento de seguridad en relación a las bases de datos en su posesión; y

XII. Elaborar contrato de transferencia, cuando se realice alguna transmisión o cesión de base de datos en su posesión;

XIII. Notificar oportunamente al Instituto, la celebración de contratos de transmisión o transferencia de datos personales a terceros;

XIV. Cada sujeto obligado deberá publicar en el Periódico Oficial del Estado la creación, modificación o supresión de los sistemas de datos personales que tengan en su posesión.

XV. Inscribir en el Sistema de Datos del Instituto, el registro de las bases de datos que tengan en su posesión;

XVI. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales;

XVII. Elaborar un plan de capacitación en materia de seguridad de datos personales;

XVIII. Resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales del titular;

XIX. Capacitar a los servidores públicos en materia de protección de datos personales en los términos de la legislación aplicable;

XX. Dar cuenta de manera fundada y motivada a la autoridad competente de la aplicación de las excepciones al régimen general para el acceso, rectificación, cancelación u oposición de datos personales;

XXI. Cumplir a cabalidad las resoluciones del Instituto; y

XXII. Las demás que se deriven de la presente ley o les señalen otros ordenamientos jurídicos aplicables.

El titular del sujeto obligado será el responsable de decidir sobre la finalidad, contenido y uso del tratamiento del sistema de datos personales, quien podrá delegar dicha atribución en la unidad administrativa en la que se concrete la

competencia material, a cuyo ejercicio sirva instrumentalmente el sistema de datos y este adscrito el responsable del mismo.

TÍTULO SÉPTIMO
DEL DOCUMENTO DE SEGURIDAD

CAPÍTULO ÚNICO
DOCUMENTO DE SEGURIDAD

Artículo 71.- Los sujetos obligados deberán elaborar un documento que establezca las medidas de seguridad físicas, técnicas y administrativas adoptadas para cada sistema de datos personales que posean, las cuales garanticen el nivel de seguridad adecuado, de conformidad al tipo de datos contenidos en dichos sistemas y con base en los estándares internacionales de seguridad y los previstos en el presente Título.

El documento de seguridad será de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los sistemas de datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas de datos personales que posea; o bien, por unidad administrativa en que se incluyan los sistemas de datos personales en custodia; o individualizado para cada sistema.

El documento de seguridad deberá incluir el nombre y cargo de los servidores públicos que intervienen en el tratamiento de datos personales con el carácter de responsable y encargado, en su caso. En el supuesto de actualización de estos datos, la modificación respectiva deberá notificarse al Instituto, dentro de los treinta días hábiles siguientes a que se efectuó.

Artículo 72.- El documento de seguridad deberá contener por lo menos lo siguiente:

I. Respecto de los sistemas de datos personales:

a) El nombre de la base de datos;

b) El nombre, cargo y adscripción del responsable y los encargados de cada sistema de datos personales, señalando, en su caso, quiénes son externos;

c) El folio de registro en el sistema desarrollado al efecto por el instituto;

d) La especificación detallada del tipo de datos personales contenidos; y

e) Estructura y descripción de la base de datos, lo cual consiste en precisar y describir el tipo del soporte, así como las características del lugar donde se resguardan.

II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente:

a) Transmisiones;

b) Resguardo de soportes físicos y/o de soportes electrónicos;

c) Bitácoras para acceso y operación cotidiana;

d) Gestión de incidentes;

e) Acceso a las instalaciones;

f) Identificación y autentificación;

g) Procedimientos de respaldo y recuperación de datos;

h) Plan de contingencia;

i) Auditorías; y

j) El procedimiento de cancelación de datos.

Artículo 73.- A efecto de facilitar el ejercicio del presente Título, los sujetos obligados deberán informar al órgano garante los documentos de seguridad en versión pública que posean, debiendo indicar, por lo menos lo siguiente:

I. La denominación de las bases de datos;

II. La normatividad aplicable que dé fundamento al tratamiento;

III. La finalidad del tratamiento;

IV. El tipo de datos personales objeto del tratamiento; y

V. La unidad administrativa que la tiene y cargo del responsable.

El documento de seguridad y demás documentación generada para la gestión de las medidas de seguridad administrativa, física y técnica tendrán el carácter de información reservada y serán de acceso restringido.

TÍTULO OCTAVO
DE EL INSTITUTODE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE NUEVO LEÓN

CAPÍTULO ÚNICO
DEL INSTITUTO

Artículo 74.- El Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales en el Estado es un órgano constitucionalmente autónomo, especializado e imparcial, con personalidad jurídica, y patrimonio propio, con autonomía presupuestaria, operativa, de decisión y de gestión, encargado de promover y difundir el ejercicio del derecho de acceso a la información, la protección de datos y resolver sobre los recursos en materia de acceso a la información pública y de datos personales.

Artículo 75.- El Instituto tendrá en materia de protección de datos personales las atribuciones siguientes:

I. Investigar, substanciar y resolver el procedimiento de inconformidad en los términos previstos en esta Ley y en la Ley de Transparencia y Acceso a la Información del Estado de Nuevo León;

II. Conocer y resolver los procedimientos que interpongan los titulares del dato, respecto de las respuestas emitidas por los sujetos obligados;

III. Vigilar el cumplimiento de las resoluciones que emita, tomando todas las medidas necesarias;

IV. Vigilar el cumplimiento de esta Ley y demás disposiciones aplicables;

V. Conocer e investigar de oficio o por denuncia, los hechos que sean o pudieran ser constitutivos de infracciones a esta Ley en materia de datos personales y, en su caso, denunciar ante las autoridades competentes, de conformidad con lo dispuesto por este ordenamiento;

VI. Establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que estén en posesión de los sujetos obligados, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta Ley;

VII. Diseñar y aprobar los formatos de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;

VIII. Establecer sistemas electrónicos para la recepción y trámite de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;

IX. Llevar a cabo el registro en forma física y sistematizada de los sistemas de datos personales en posesión de los sujetos obligados;

X. Elaborar y mantener actualizado el registro del nivel de seguridad aplicable a los sistemas de datos personales, en posesión de los sujetos obligados, en términos de esta Ley;

XI. Emitir opiniones sobre temas relacionados con la presente Ley, así como formular observaciones y recomendaciones a los sujetos obligados, derivadas del incumplimiento de los principios que rigen esta Ley;

XII. Orientar y asesorar a las personas que lo requieran acerca del contenido y alcance de la presente ley;

XIII. Elaborar y publicar estudios e investigaciones para difundir el conocimiento de la presente Ley;

XIV. Solicitar y evaluar los informes presentados por los sujetos obligados respecto del ejercicio de los derechos previstos en esta Ley. Dicha evaluación se incluirá en el informe que de conformidad a la Ley de Transparencia y Acceso a la Información presenta el Instituto al H. Congreso del Estado.

XV. Organizar seminarios, foros, cursos, talleres y demás actividades que promuevan el conocimiento de la presente Ley y los derechos de las personas sobre sus datos personales;

XVI. Establecer programas de capacitación en materia de protección de datos personales y promover acciones que faciliten a los sujetos obligados y a su personal participar de estas actividades, a fin de garantizar el adecuado cumplimiento de los principios que rigen la presente Ley;

XVII. Promover entre las instituciones educativas, públicas y privadas, la inclusión dentro de sus actividades académicas curriculares y extracurriculares, los temas que ponderen la importancia del derecho a la protección de datos personales;

XVIII. Promover la elaboración de guías que expliquen los procedimientos y trámites materia de esta Ley;

XIX. Procurar la conciliación de los intereses de los interesados con los de los sujetos obligados, cuando éstos entren en conflicto con motivo de la aplicación de la presente Ley;

XX. Llevar a cabo visitas de verificación en materia de seguridad de datos personales en posesión de los sujetos obligados;

XXI. Investigar las posibles violaciones a las disposiciones de esta Ley; y

XXII. Promover y difundir de manera permanente la cultura de la protección de datos personales;

XXIII. Impulsar conjuntamente con instituciones de educación, la integración de centros de investigación, difusión y docencia sobre el derecho de protección de datos personales, que promuevan el conocimiento sobre este tema y coadyuven con el Instituto en sus tareas sustantivas;

XXIV. Establecer un sistema que garantice y haga efectivo el adecuado y pleno ejercicio de los derechos de protección de datos personales;

XXV. Celebrar convenios con autoridades federales, estatales o municipales;

XXVI. Celebrar convenios con organismos nacionales e internacionales, así como de la sociedad civil;

XXVII. Celebrar convenios para allegarse recursos financieros;

XXVIII. Mantener una efectiva colaboración y coordinación con los sujetos obligados, a fin de lograr el cumplimiento de esta Ley; y

XXIX. Las demás que establezca esta Ley, y demás ordenamientos aplicables.

Artículo 76.- Las resoluciones que emita este Instituto deberán estar fundadas y motivadas y podrán sobreseer o desechar el recurso de revisión por improcedente; o confirmar, revocar o modificar la respuesta o resolución del sujeto obligado.

TÍTULO NOVENO
DEL RECURSO DE REVISIÓN
CAPÍTULO ÚNICO
RECURSO DE REVISIÓN

Artículo 77.- El titular del dato o su representante legal, podrá interponer el recurso de revisión, de manera directa o por medios electrónicos, ante el Instituto o ante el sujeto obligado que haya conocido del asunto, en este último caso se deberá notificar de manera inmediata y por cualquier medio al Instituto sobre la interposición del recurso y remitir el documento dentro de los tres días hábiles siguientes de haberlo recibido.

El sujeto obligado al momento de dar respuesta a una solicitud de acceso, rectificación, cancelación u oposición de datos personales, deberá orientar al particular sobre su derecho de interponer el recurso de revisión y el modo de hacerlo, especialmente cuando el titular no sepa leer ni escribir, hable una lengua indígena, se trate de una persona que pertenezca a un grupo vulnerable, o bien cuando no sepa que documentos contiene la información de su interés.

Artículo 78.- El recurso de revisión procede por cualquiera de las siguientes causas:

I. La negativa de acceso, rectificación, cancelación u oposición de datos personales;

II. El sujeto obligado no entregue los datos personales solicitados, o lo haya hecho en formato incomprensible;

III. El solicitante considere que la información entregada es incompleta o no corresponda a la información requerida en la solicitud;

IV. El tratamiento inadecuado de los datos personales;

V. El solicitante no esté conforme con el tiempo o costo;

VI. La entrega de información en una modalidad distinta a la solicitada;

VII. La inconformidad con las razones que motivan una prórroga;

VIII. La negativa de acceso, rectificación, cancelación u oposición de datos personales;

IX. El tratamiento inadecuado de los datos personales;

X. La declaración de incompetencia de un sujeto obligado;

XI. El desechamiento de la solicitud de los derecho de acceso, rectificación, cancelación y oposición en los términos de la Ley de Transparencia y Acceso a la Información del Estado de Nuevo León;

XII. Cuando no se hayan revocado sus datos personales; y

XIII. La negativa ficta.

Se actualizará la negativa ficta, cuando dentro de los plazos establecidos en esta Ley, el sujeto obligado no diera respuesta a una solicitud de acceso, rectificación, cancelación u oposición de datos personales.

Artículo 79.- El recurso deberá interponerse dentro de los quince días siguientes a la notificación correspondiente o en su caso, a partir del momento en que hayan transcurrido los términos establecidos para dar contestación a las solicitudes de acceso, rectificación, cancelación, revocación o de oposición de datos personales, supuestos en que bastará que el titular del dato, representante o mandatario legal acompañe al procedimiento el documento que prueba la fecha en que se presentó la solicitud.

Artículo 80.- El recurso de revisión podrá interponerse por escrito libre, a través de los formatos que al efecto proporcione el Instituto o por medios electrónicos, debiendo contener y anexar lo siguiente:

I. El nombre del titular del dato y en su caso, el de su representante legal o mandatario, que cumpla con las formalidades de Ley y el del tercero interesado si lo hubiera, de lo contrario, precisar la inexistencia del mismo;

II. El sujeto obligado ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales o revocación;

III. El domicilio o medio electrónico del titular del dato, el de su representante legal o mandatario y el del tercero interesado, si lo hubiera, para efectos de oír y recibir notificaciones; en caso de no haber señalado el titular del dato, aún las de carácter personal, se harán por tabla de avisos;

IV. El acto o resolución del cual se inconforma y, en su caso, el número de expediente que identifique el mismo;

V. La fecha en que se le notificó o tuvo conocimiento del acto reclamado, salvo que el procedimiento se interponga por la falta de respuesta a una solicitud de acceso a información, o de acceso, rectificación, cancelación u oposición de datos personales;

VI. Los puntos petitorios;

VII. El documento con el que acredita la existencia de la solicitud y el documento con el que se acredite la respuesta emitida por el sujeto obligado, en su caso;

VIII. Los documentos que acrediten la personalidad del titular, representante legal o mandatario; y

IX. Las demás pruebas y elementos que se considere procedente hacer del conocimiento del Instituto.

En el caso de que el recurso se interponga a través de medios que no sean electrónicos, deberá acompañarse de las copias de traslado suficientes.

Artículo 81.- Se considera como tercero o terceros interesados a:

I. La persona o personas distintas al promovente del Recurso de Revisión, que sea parte dentro de un juicio o procedimiento del cual se solicite la información;

II. La persona o personas distintas al promovente del Recurso de Revisión, que justifique tener interés directo en mantener la reserva o confidencialidad de la información solicitada.

Artículo 82.- En todos los casos, el Instituto deberá suplir las deficiencias del recurso de revisión, siempre y cuando no altere el contenido original de la solicitud, ni se modifiquen los hechos o peticiones expuestos en dicho recurso.

Artículo 83.- En caso de que el recurso de revisión no satisfaga alguno de los requisitos a que se refiere el artículo 80 de esta Ley, y el Instituto no cuente con elementos para subsanarlo, prevendrá al particular dentro los cinco días hábiles días hábiles siguientes a la interposición de dicho recurso, por una sola ocasión, para que subsane las omisiones dentro de un plazo de cinco días hábiles. Transcurrido el plazo sin desahogar la prevención se tendrá por no presentado el recurso.

La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver el recurso.

Artículo 84.- Presentado el recurso de revisión ante el Instituto, se estará a lo siguiente:

I. Se turnará a uno de los Comisionados quien será el encargado de dar trámite a todo el recurso, así como presentar ante el Pleno el proyecto de resolución respectivo;

II. El auto de admisión se dictará al día hábil siguiente al de la presentación del recurso;

III. Admitido el recurso, se integrará un expediente y se notificará al sujeto obligado señalado como responsable, para que dentro del término de cinco días hábiles contados a partir del día siguiente de dicha notificación, ofrezca su contestación y aporte las pruebas que considere pertinentes;

IV. En el caso de existir tercero interesado en los términos que dispone la presente Ley, se le hará la notificación para que en el plazo de cinco días hábiles, alegue lo que a su derecho convenga y presente las pruebas que considere pertinentes;

V. Recibida la contestación o transcurrido el plazo para contestar el recurso de revisión, el Instituto dentro de un plazo de tres días hábiles deberá citar a las partes a una Audiencia de Conciliación en la cual, de llegar a un acuerdo satisfactorio, éste tendrá efectos vinculantes para las partes, suspendiéndose el trámite del recurso durante el término que dure la conciliación.

En caso de que se cumpla el acuerdo antes mencionado, se emitirá la resolución correspondiente, y en el supuesto de incomparecencia de alguna de las partes, por no llegar a un acuerdo favorable entre las mismas, o por incumplimiento de dicho acuerdo, se continuará con la secuela procesal y se dará vista dará vista al particular para que en un plazo de cinco días hábiles y alegue lo que a su derecho convenga;

VI. Si alguna de las partes ofrece medios de prueba que requieran de desahogo o de algún trámite para su perfeccionamiento, el Instituto determinará

audiencias con el titular del dato y/o representante legal y el sujeto obligado, dentro de los tres días hábiles siguientes a que se recibieron. Una vez desahogadas las pruebas se declarará cerrada la instrucción y el expediente se encontrará en estado de resolución;

VII. Excepcionalmente, el Instituto podrá ampliar los plazos hasta por diez días hábiles más cuando la importancia y trascendencia del asunto así lo amerite; y

VIII. Cerrada la instrucción, el Pleno de la Comisión, bajo su más estricta responsabilidad, deberá emitir una resolución debidamente fundada y motivada, en un término no mayor de diez días hábiles, contados a partir de que el expediente se encuentre en estado de resolución.

Artículo 85.-La Acumulación de dos o más recursos podrá solicitarse a instancia de parte o de oficio, en cualquier momento del procedimiento, hasta antes de que se cierre la instrucción y se ponga en estado de resolución.

Artículo 86.- La Acumulación será procedente cuando las partes sean las mismas y se invoquen idénticos actos.

Artículo 87.- La Acumulación se tramitara ante el Comisionado Ponente que esté conociendo del recurso primeramente promovido, y éste a su vez en un término de tres días hábiles resolverá lo procedente.

Decretada la Acumulación se suspenderá el curso del recurso que estuviere más próximo a resolverse, hasta que el otro se encuentre en el mismo estado, a fin de que ambos se decidan en una misma resolución.

Artículo 88.- Para la consecución de la verdad y la justicia que constituyen un interés fundamental y común de las partes, el Comisionado Ponente a quien se le haya turnado para su substanciación un Recurso de Revisión, Denuncia o Asunto diverso, podrá en todo tiempo ordenar que se subsane toda omisión que notare en la substanciación del recurso, así mismo, y con independencia de los elementos de convicción que rindan las partes, decretará la práctica de cualquier diligencia, la aportación o ampliación de pruebas que se estime necesarias y conducentes a

aquellos objetivos, sin más limitación que sean de las reconocidas por la presente Ley y que tengan relación con los hechos controvertidos.

Artículo 89.- La información confidencial o reservada que, en su caso, sea solicitada por el Instituto por resultar indispensable para resolver el asunto, deberá ser mantenida con ese carácter y no estará disponible en el expediente.

Artículo 90.-La falta de contestación del sujeto obligado al Recurso de Revisión dentro del término establecido en la presente Ley, hará presumir como ciertos los hechos que se hubieren señalado en él, siempre que éstos le sean directamente imputables. En estos casos el plazo para resolver el procedimiento será de diez días hábiles.

Artículo 91.- Las partes y el tercero interesado podrán ofrecer únicamente como pruebas de su intención las documentales públicas, documentales privadas, testigos, fotografías, copias fotostáticas, cintas de vídeo, dispositivos de archivos electrónicos o magnéticos, registros dactiloscópicos, electrónicos y, en general, todos aquellos elementos derivados de los avances de la ciencia y la tecnología y presuncionales. El desahogo y la calificación de las mismas, así como las notificaciones se realizarán aplicando supletoriamente el Código de Procedimientos Civiles del Estado de Nuevo León. En cualquier caso, corresponderá a la Comisión desechar de plano aquellas pruebas que no guarden relación con el recurso.

Artículo 92.- Interpuesto el Recurso de Revisión por una negativa ficta y una vez admitido a trámite, el Instituto dará vista al sujeto obligado para que, en un plazo no mayor a tres días hábiles, acredite haber respondido en tiempo y forma la solicitud, o bien dé respuesta a la misma.

En el primer caso, el recurso se considerará improcedente y el Instituto deberá dictar auto de sobreseimiento en un término de 48 horas. En el segundo caso, el Instituto emitirá, en un plazo no mayor de cinco días hábiles su resolución, con base en el contenido de la solicitud original y la respuesta del sujeto obligado. La falta de contestación del sujeto obligado al recurso de revisión por negativa ficta

dentro del término establecido, en el presente artículo, hará presumir como ciertos los hechos que se hubiera señalado en él, siempre que éstos le sean directamente imputables.

Si la resolución del Instituto determina la procedencia de otorgar el acceso, rectificación, cancelación o la oposición al tratamiento de sus datos personales solicitados, se procederá a su entrega, según corresponda al derecho que haya solicitado.

Artículo 93.- Las resoluciones del Instituto podrán:

I. Sobreseer o desechar el Recurso de Revisión por improcedente;

II. Confirma, revocar o modificar la respuesta o resolución del sujeto obligado, por lo que deberá ordenar el acceso, rectificación, cancelación u oposición de datos personales.

Artículo 94.- Los sujetos obligados deberán cumplir con las resoluciones, bajo los siguientes lineamientos:

I. En caso de que el cumplimiento derive en el cobro de derechos por la modalidad solicitada, el sujeto obligado deberá hacer del conocimiento del particular el concepto, cantidad y lugar de pago, dentro de los cinco días hábiles siguientes a la fecha en que haya quedado notificada la resolución; así mismo el particular contará con un término de cinco días hábiles para realizar el pago correspondiente y hacerlo del conocimiento al sujeto obligado y el propio sujeto obligado deberá hacer entrega de la información en un término de diez días hábiles contados a partir de aquel en que se exhiba el pago de derechos;

II. Cuando para la entrega o acceso, rectificación, cancelación u oposición de los datos no se requiera pago alguno, el sujeto obligado deberá proporcionarla o permitirla en un término no mayor de cinco días hábiles, contados a partir de la fecha en que haya quedado notificada la resolución;

III. Para el caso del examen de algún objeto, documento o cualquier otra forma de registro ordenada, el sujeto obligado deberá señalar lugar, fecha y hora dentro del término de cinco días hábiles siguientes a la fecha en que haya quedado notificada la resolución, mismo que deberá celebrarse en un plazo que no exceda de cinco días hábiles posteriores;

IV. Los sujetos obligados, en su caso, deberán informar al Instituto del cumplimiento de sus resoluciones, en un plazo no mayor a cinco días hábiles posteriores a aquel en que se les notificó la resolución, a menos que en la misma el Instituto determine un plazo mayor para su cumplimiento;

V. En todo lo no previsto en las fracciones anteriores, el Instituto determinará lo correspondiente.

Artículo 95.- El sujeto obligado al rendir su contestación dentro del recurso de revisión, deberá designar un domicilio ubicado en cualquier municipio del área metropolitana de Monterrey o medio electrónico, para efectos de oír y recibir notificaciones. En caso de que no cumpla con dicha prevención, las notificaciones que conforme a las reglas generales deben hacerse personalmente, se le harán por medio de la tabla de avisos con que cuenta este organismo autónomo.

Artículo 96.- Las actuaciones del Instituto se notificarán, en el domicilio o medio electrónico que al efecto señalen las partes o en su defecto en la tabla de avisos, al día hábil siguiente en que se dicten y surtirán efectos un día hábil después, contándose para ello el día del vencimiento. Las resoluciones deberán notificarse a las partes y publicarse a más tardar al tercer día siguiente de su aprobación o engrose.

Artículo 97.- En caso de incumplimiento de la resolución del recurso de revisión, el Instituto notificará al superior jerárquico del sujeto obligado responsable a fin de que ordene el cumplimiento en un plazo que no excederá de tres días hábiles.

En caso de persistir el incumplimiento, el Instituto dará vista al órgano interno de control del sujeto obligado para que verifique el mismo y, en su caso, éste proceda

a sancionar al presunto responsable. Lo anterior sin perjuicio de que el particular haga valer sus derechos ante las instancias judiciales correspondientes.

Artículo 98.- No podrá archivarse ningún expediente sin que se haya cumplido la resolución correspondiente ni se hubiere extinguido la materia de la ejecución.

Artículo 99.- Todas las resoluciones del Instituto serán públicas, salvo cuando contengan información clasificada, en cuyo caso se elaborarán versiones públicas.

Artículo 100.- El recurso de revisión será desechado por improcedente cuando:

I. El Instituto no sea competente;

II. El Instituto haya conocido anteriormente del recurso de revisión contra el mismo acto y resuelto en definitiva respecto del mismo recurrente;

III. Sea extemporánea;

IV. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular o su representante legal que pueda tener por efecto modificar o revocar el acto respectivo;

V. Se impugnen actos o resoluciones que no hayan sido emitidos por el sujeto obligado;

VI. El sujeto obligado hubiere acreditado haber respondido en tiempo y forma la solicitud de información; o

VII. Se recurra una resolución, acto o respuesta que no hayan sido emitidos por el sujeto obligado.

Artículo 101.- El recurso de revisión será sobreseído cuando:

I. El titular fallezca;

II. El titular se desista de manera expresa del recurso interpuesto;

III. Admitido el recurso, sobrevenga una causal de improcedencia;

IV. Ante la manifestación expresa de la conformidad con el acceso, rectificación, cancelación, oposición y revocación de los datos personales del titular del dato; y

V. Por cualquier motivo quede sin materia el Recurso de Revisión.

Artículo 102.- A fin de que la tramitación del procedimiento de inconformidad sea expedita, el Instituto podrá aplicar las siguientes medidas de apremio, previa la audiencia del sujeto obligado:

I. Apercibimiento;

II. Amonestación privada;

III. Amonestación pública; y

IV. Multa de 200 a 1500 cuotas.

Artículo 103.- Cuando la Ley no señale término alguno, se tendrá por señalado el de tres días hábiles.

Artículo 104.- Todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, siempre y cuando la resolución de referencia se someta a un proceso de disociación, es decir, no haga identificable al titular del dato.

TÍTULO DÉCIMO
DE LAS RESPONSABILIDADES Y SANCIONES

CAPÍTULO ÚNICO
RESPONSABILIDADES Y SANCIONES

Artículo 105.- Los sujetos obligados, incurrirán en responsabilidad administrativa leve, sin perjuicio de las del orden penal o civil que correspondan, por incumplimiento de las obligaciones establecidas a continuación:

I. Por falta de nombramiento oportuno de los responsables y encargados de la protección de datos personales;

II. Por omitir publicar o poner a disposición de las personas titulares de datos personales, total o parcialmente, el aviso de privacidad;

III. Por no inscribir oportunamente las bases de datos personales, en el registro que para tal efecto lleva el Instituto;

IV. Por declarar con dolo, negligencia o mala fe, la inexistencia de datos personales, cuando estos existan total o parcialmente en sus archivos;

V. Por no dar respuesta oportuna a las solicitudes de protección de datos personales, o bien, por no comunicar al titular del dato la falta de competencia del sujeto obligado;

VI. Por entregar información relativa a datos personales, de manera errónea o incompleta, requerida en una solicitud de protección de datos personales;

VII. Por actuar con negligencia, dolo o mala fe, en la debida sustanciación de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

VIII. Por no rendir en tiempo y forma, contestación a un procedimiento de inconformidad interpuesto en el ejercicio de los derechos de protección de datos personales.

IX. Por falsas causales de prórroga o ampliación del plazo para contestar solicitudes que supongan negligencia o descuido; y

X. Por no informar a los titulares una transmisión de datos, dentro de los diez días hábiles siguientes a dicha cesión.

XI. Por no informar de manera fehaciente al titular del dato del derecho que tiene de interponer el Recurso de Revisión ante este Instituto; al emitir la contestación a la solicitud de los derechos de Acceso, Rectificación, Cancelación y Oposición.

Artículo 106.- Los sujetos obligados descritos en la presente Ley, incurrirán en responsabilidad administrativa grave, sin perjuicio de las del orden penal o civil que correspondan, por incumplimiento de las obligaciones establecidas a continuación:

I. Por incumplir con el deber de secreto y confidencialidad a que está obligado;

II. Por transgredir las medidas de protección y confidencialidad a que se refiere la presente Ley;

III. Por cambiar sustancialmente la finalidad originaria del tratamiento de datos personales;

IV. Por proceder a la recolección y transmisión de datos de carácter personal, sin contar con el debido consentimiento expreso y por escrito de sus titulares, siempre que proceda;

V. Por no notificar o respetar la garantía de audiencia, en el trámite de una solicitud de información que contenga datos personales de persona distinta al titular, representante o mandatario legal;

VI. Por mantener datos de carácter personal inexactos, siempre que resulte imputable a los sujetos obligados, al no efectuar las rectificaciones o cancelaciones de los mismos;

VII. Por incumplir las medidas de seguridad y protección de las bases de datos personales determinados en la presente Ley, y en los lineamientos expedidos por el Instituto;

VIII. Por impedir, obstaculizar o negar indebidamente el ejercicio de los derechos de protección de los datos personales;

IX. Por no notificar oportunamente al Instituto, la celebración de contratos de transmisión o transferencia de datos personales a terceros; y

X. Por clasificar o confirmar indebidamente una clasificación de información confidencial, con dolo, negligencia o mala fe, cuando no cumpla con las

características que señala esta Ley, o la Ley de Transparencia y Acceso a la Información del Estado. Esta causal solo procederá cuando exista una resolución previa del Instituto, respecto del criterio de clasificación.

Artículo 107.- Los sujetos obligados descritos en esta Ley, incurrirán en responsabilidad administrativa muy grave, sin perjuicio de las del orden penal o civil que correspondan, por incumplimiento de las obligaciones establecidas a continuación:

I. Por crear, transmitir, tratar, usar, sustraer, destruir, ocultar, inutilizar, divulgar, alterar o modificar total o parcialmente de manera indebida, datos personales a los cuales tenga acceso, o bien, se encuentren bajo su custodia o posesión;

II. Por ordenar o facilitar a terceros, información confidencial que obre en sus archivos o sistemas de datos personales, sin la existencia debida del contrato de transmisión;

III. Por la planeación de cualquier acto, que implique la indebida transmisión de las bases de datos personales por cualquier medio, con fines específicos de obtener un lucro indebido;

IV. Por la creación de bases de datos personales sensibles, prohibidos por la presente Ley;

V. Por ordenar o facilitar la entrega de una resolución judicial , electoral o administrativa, sin la debida supresión de los datos considerados confidenciales;

VI. Por no proporcionar oportunamente la información que solicite el Instituto, en el ejercicio de sus competencias legales;

VII. Por impedir u obstaculizar de cualquier forma, el ejercicio debido de las facultades de protección de datos personales del Instituto;

VIII. Por incumplir u obstaculizar de cualquier forma, las resoluciones emitidas por el Instituto;

IX. Por no cesar en el uso ilegitimo o ilícito de los tratamientos de datos personales, por requerimiento del Instituto; y

X. Por la transmisión de datos considerados confidenciales, en el caso de archivos de Seguridad Pública, Fiscal, Judicial o de Salud.

Artículo 108.- Las responsabilidades a que se refiere este artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada por el superior jerárquico del servidor público presunto responsable siguiendo los procedimientos establecidos en la Ley de Responsabilidades de los Servidores Públicos del Estado y Municipios de Nuevo León.

Las resoluciones finales que al respecto expidan los órganos internos de control o sus equivalentes deberán ser notificadas al Instituto, quien deberá hacerlas públicas a través del informe anual a que se refiere la Ley de Transparencia y Acceso a la Información del Estado de Nuevo León.

Artículo 109.- El Instituto podrá imponer las siguientes sanciones económicas al sujeto obligado, de conformidad al tipo de infracción que haya cometido, señaladas en los artículos anteriores, de la siguiente manera:

I. Las infracciones señaladas como leves, serán sancionadas con multa de 100 a 500 cuotas;

II. Las infracciones señaladas como graves, serán sancionadas con multa de 501 A 1,000 cuotas; y

III. Las infracciones señaladas como muy graves serán sancionas con multa de 1,001 a 10, 000 cuotas.

Toda multa o sanción de carácter económico impuesta por el Instituto, se entenderá a cargo del patrimonio personal del servidor público sancionado.

a) En caso de reincidencia o desacato a una resolución, el Instituto podrá solicitar al superior jerárquico del servidor público responsable o a las autoridades competentes;

- El inicio del procedimiento de separación temporal del responsable, hasta por seis meses;

- La separación definitiva del responsable; o

- La inhabilitación del cargo del servidor público, hasta por cinco años, de conformidad con los procedimientos establecidos por la Ley de Responsabilidades de los Servidores Públicos del Estado y Municipios de Nuevo León. En caso de que el incumplimiento sea realizado por autoridad que goce de fuero constitucional, se procederá en los términos que señale la ley de la materia.

Artículo 110.- Las sanciones se aplicarán de conformidad con los siguientes criterios:

I. La individualización de la sanción en relación a la capacidad económica del sujeto obligado infractor;

II. La gravedad de la falta cometida y la conveniencia de suprimir prácticas que atenten contra la protección de datos;

III. Las circunstancias y condiciones del incumplimiento a la Ley;

IV. La reincidencia por parte del sujeto obligado en el incumplimiento a las obligaciones en materia de protección de datos. Se considerará reincidente el sujeto obligado que incurra más de una vez en alguna o algunas de las conductas que se señalan en los artículos 106, 107 y 108 de la presente Ley;

V. El carácter intencional o negligente de la acción u omisión constitutiva de la falta cometida por el sujeto obligado; y

VI. El monto del beneficio o daño o perjuicio económico derivado del incumplimiento.

Artículo 111.- El Instituto podrá presentar denuncias ante las autoridades competentes por cualquier conducta prevista en el artículo 105, 106 y 107 de esta Ley y aportar las pruebas que considere pertinentes.

Artículo 112.- El Instituto remitirá mediante oficio a la Secretaría de Finanzas y Tesorería General del Estado, las sanciones impuestas a los sujetos obligados, las cuales tendrán el carácter de créditos fiscales, para efecto que lleve a cabo las acciones legales de ejecución, la cual estará obligada a presentar informes mensuales del estado que guarda la ejecución de las multas al Instituto.

ARTÍCULOS TRANSITORIOS

Primero.- La presente Ley entrará en vigor treinta días hábiles después de su publicación en el Periódico Oficial del Gobierno del Estado de Nuevo León.

Segundo.- El Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Nuevo León, expedirá el Reglamento de esta Ley, dentro de los noventa días hábiles posteriores a la entrada en vigor de la presente Ley.

Tercero.- Los sujetos obligados que administren sistemas de datos personales, deberán registrar ante el Instituto la relación de los Sistemas de Datos Personales, dentro de los treinta días hábiles posteriores a la entrada en vigor de la presente Ley.

Cuarto.- Los titulares u órganos de gobierno de los sujetos obligados, designarán a la persona responsable del sistema de datos personales, dentro de los treinta días hábiles posteriores a la entrada en vigor de este ordenamiento legal.

Quinto.- Las solicitudes y el procedimiento de inconformidad en trámite a la entrada en vigor de esta Ley se resolverán conforme a la Ley de Transparencia y Acceso a la Información del Estado.

Los recursos de revisión que sean presentados a partir de la entrada en vigor de esta Ley, se regirán, por lo que hace al procedimiento, por las disposiciones de la misma, y por lo que hace a la materia sustantiva, por las disposiciones vigentes al momento en que fue presentada la solicitud de información que originó el acto de inconformidad.

Sexto.- Las Autoridades en materia judicial, electoral o administrativa del Estado, deberán expedir los reglamentos o acuerdos generales a que se refiere el artículo 55 de esta Ley, en un periodo de sesenta días hábiles después de la entrada en vigor de la presente Ley.

Séptimo.- En relación al documento de seguridad que regula el artículo 73 de la presente Ley; los sujetos obligados deberán elaborar el documento que establezca las medidas de seguridad físicas, técnicas y administrativas adoptadas para cada sistema de datos personales, en un periodo de treinta días hábiles después de la entrada en vigor de la presente Ley.

Octavo. En relación al documento de seguridad en versión pública; los sujetos obligados deberán remitirlo al Instituto en un lapso de 120 días hábiles después de la entrada en vigor de la presente Ley.

ATENTAMENTE

Monterrey, Nuevo León a febrero de 2015-dos mil quince

Lic. Sergio Mares Moran

Comisionado Presidente

Lic. Sergio Antonio Moncayo González
Comisionado Vocal

Ing. Juan de Dios Villarreal González
Comisionado Vocal

Lic. María Eugenia Pérez Eimbcke
Comisionada Supernumeraria
en su calidad de Secretario de Actas

12.31 h.

H. CONGRESO DEL ESTADO
OFICIALIA MAYOR
RECIBIDO
10 FEB 2015
DEPARTAMENTO
OFICIALIA DE PARTES
MONTERREY, N. L.