LXII LEGISLATURA
ESTADO DE ZACATECAS
2016 • 2018

DICTAMEN DE LA COMISIÓN LEGISLATIVA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, RESPECTO DE LAS INICIATIVAS CON PROYECTO DE DECRETO POR LAS QUE SE EMITE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS DEL ESTADO DE ZACATECAS.

HONORABLE ASAMBLEA:

A la Comisión Legislativa de Transparencia y Acceso a la Información Pública le fueron turnadas, para su estudio y dictamen, sendas iniciativas con proyecto de Decreto por las que se emite la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Zacatecas, que presentaron la diputada Julia Arcelia Olguín Serna y el diputado Jorge Torres Mercado.

Vistas y estudiadas que fueron las iniciativas en cita, esta Comisión Legislativa somete a la consideración del Pleno el presente Dictamen, con base en los siguientes

A N T E C E D E N T E S:

PRIMERO. En sesión ordinaria de la Comisión Permanente de esta Soberanía Popular, celebrada el 21 de febrero de 2017, se dio lectura a la iniciativa con proyecto de decreto por el que se expide la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Zacatecas, que presentó la diputada Julia Arcelia Olguín Serna, con fundamento en los artículos 60 fracción I de la Constitución Política del Estado de Zacatecas; 46 fracción I y 48 fracción II de la Ley Orgánica del Poder Legislativo del Estado y 95 fracción I de su Reglamento General.

SEGUNDO. En esa misma fecha, por acuerdo de la Presidencia de la Mesa Directiva, la iniciativa referida fue turnada mediante memorándum número 0424 a esta Comisión Legislativa, para su estudio y dictamen correspondiente.

TERCERO. La diputada proponente justificó su iniciativa en la siguiente

EXPOSICIÓN DE MOTIVOS

El derecho al acceso a la información ha sido una conquista de los ciudadanos conjuntamente con el derecho inherente de la transparencia del ejercicio del quehacer público en nuestro país. Estos derechos se tipifican en un conglomerado de disposiciones legislativas que conforman el marco jurídico en materia de acceso a la información pública, protección de datos personales y archivos, publicado en el Diario Oficial de la Federación el 7 de febrero de 2014. Así mismo, este marco

jurídico se ve completado con la publicación en el Diario Oficial de la Federación el 4 de mayo de 2015, de la Ley General de Transparencia y Acceso a la Información.

Posteriormente y siguiendo dicho ordenamiento, el Estado de Zacatecas asumió lo mandatado en dicha Ley General habiendo legislado la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas; ésta última sería publicada en el suplemento 5 del Periódico Oficial No. 44 del Estado de Zacatecas, el 02 de junio de 2016.

Cabe destacar que tanto la Ley General como la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas, dan cuenta que nuestra Carta Magna enuncia que la protección de datos personales es un derecho humano de las personas. Por tal motivo, se da pauta para que dichas Leyes puedan ser fortalecidas por futuras normas comunicantes en materia de protección de datos personales en posesión de sujetos obligados.

Un sujeto obligado se entiende por cualquier autoridad, entidad, órgano y organismos de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos; mismos que por sus acciones cotidianas uno de sus principales insumos de información son precisamente datos personales de los ciudadanos. Es menester entonces regular el trato que se le da a este tipo de información desde el ámbito público puesto que dicha información sin ningún tipo de regulación se vuelve gravemente vulnerable pudiendo atentar directamente sobre la integridad de personas físicas y morales. Lo anterior, referido en el artículo 6 párrafo A Fracción I de la Constitución Política de los Estados Unidos Mexicanos:

"*Toda la información en posesión de cualquier autoridad, entidad, 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 federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicada. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información. De igual manera es primordial que los sujetos responsables del manejo de datos personales en posesión de sujetos obligados observen los principios de licitud, finalidad, lealtad, consentimientos, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los mismos*"[1].

[1] Constitución Política de los Estados Unidos Mexicanos. Artículo 6.

De esta manera y con el fin de concretar el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales que prevé la Ley General de Transparencia y Acceso a la Información surge la imperante necesidad de legislar en materia de protección de datos personales en posesión de sujetos obligados. Podemos señalar cómo el artículo 68 de la Ley General ya hace un llamamiento para legislar en materia de protección de datos personales en posesión de sujetos obligados:

Art. 68 Los sujetos obligados serán responsables de los datos personales en su posesión y, en relación con éstos deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso, rectificación, corrección y oposición al tratamiento de datos, en los casos que sea procedente, así como capacitar a los Servidores Públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con la normativa aplicable.

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales hayan sido obtenido o dicho tratamiento se haga en ejercicio de las atribuciones conferidas por ley.

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezca los propósitos para su tratamiento, en términos de la normatividad aplicable, excepto en casos en que el tratamiento de los datos se haga en ejercicio de las atribuciones conferidas por ley.

IV. Procurar que los datos personales sean exactos y actualizados.

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación.

VI. **Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado**. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo a la normatividad aplicable. Lo anterior, sin perjuicio a lo establecido por el artículo 120 de esta Ley.[2]

[2] Ley General de Transparencia y Acceso a la Información Pública. (Fecha de consulta: 30 de enero de 2017)

Agreguemos que nuestra Carta Magna en sus artículos 6 y 16, sustenta las bases para una construcción normativa en materia de datos personales:

Art. 6. …

I. …

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, ***a sus datos personales o a la rectificación de estos****.*

IV. …

V. …

VI. …

VII. …

VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad de decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la Ley. El organismo autónomo previsto en esta fracción, se seguirá por la ley en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados, en los términos que establezca la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba ye ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de quienes asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros. También conocerá de los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de las entidades federativas que determinen la reserva,

confidencialidad, inexistencia o negativa de la información, en los términos que establezca la Ley.

Art. 16. *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como de manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamientos de datos, por razones de seguridad nacionales, disposición es de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

Así, queda de manifiesto que el uso de datos personales en posesión de sujetos obligados exige una normativa propia, que dentro de la constitucionalidad, regule los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) que constituyen los cuatros pilares del derecho humano entorno a la protección de datos personales y que se ostentan en el artículo 6 de nuestra Carta Magna que dice:

"Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos".

Sólo como referencia, sería prudente mencionar que en el ámbito internacional podemos encontrar legislaciones precedentes que ratifican dichos derechos ARCO, tal es el caso del Reglamento del Parlamento Europeo que en su Considerando 32 se menciona que:

"El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".[3]

[3] Diario Oficial de la Unión Europea. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento

Con toda la anterior referencia, en el caso de México, sería el 28 de abril de 2016 cuando las Comisiones Unidas de Gobernación y de Estudios Legislativos del Senado de la República aprobaron el Dictamen con proyecto de decreto que expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[4]. Siguiendo el procedimiento legislativo, el 3 de mayo de 2016 dicha Minuta se publicó en la Gaceta Parlamentara de la Cámara de Diputados, misma que fue turnada a la Comisión de Transparencia y Anticorrupción para dictamen y a la Comisión Especial de las Tecnologías de la Información y Comunicación para su opinión.

Es de reconocimiento que dicha Comisión de Transparencia y Anticorrupción coadyuvó esfuerzos con representantes de la sociedad civil y la academia a fin de nutrir y perfeccionar el contenido la Minuta en cuestión. Así mismo, por referirse a una legislación de un derecho humano, dicha Minuta sería sometida a un test de proporcionalidad en sentido amplio; esto significaba que la Minuta o Proyecto Legislativo debía confirmar que perseguía una finalidad constitucionalmente válida; debía lograr un grado a la consecución de su fin; no debía de limitar de manera innecesaria y desproporcionada el derecho humano referido y finalmente, debía pasar por un examen estricto de proporcionalidad en sentido estricto donde se comparara el grado de intervención en el derecho fundamental respecto al grado de realización del fin perseguido.

El 30 de noviembre de 2016, la Comisión de Transparencia y Anticorrupción de la Cámara de Diputados y después de haber recibido una opinión positiva de parte de la Comisión Especial de las Tecnologías de la Información y Comunicación, aprobaría en lo general el Dictamen con relación a la Minuta con Proyecto de Decreto por el que se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Finalmente, dicho Dictamen sería aprobado el 13 de Diciembre de 2016 dando origen a la Ley General de Protección de Datos Personales en Posesión de Sujetos misma que entraría en vigor el pasado 27 de enero de 2017.

Si bien lo anterior se refiere al ámbito federal, en el aspecto local, cabe señalar que Zacatecas publicó su primera Ley de Transparencia y Acceso a la Información Pública en junio de 2011 misma que sería abrogada en junio de 2016 por una nueva Ley en la materia que actualizó y modernizó toda la normativa para estar en apego a la Ley General. Dentro de la armonización de la Ley del Estado con la Ley Federal,

---

de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Agencia Española de Protección de Datos. https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf (Fecha de consulta 30 de enero de 2017).

[4] Senado de la República. Dictamen de las Comisiones Unidades de Gobernación y de Estudios Legislativos Primera, con proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados . (Fecha de consulta 1 de febrero de 2017)

quedó asentado en la primera, en su artículo sexto transitorio, que mientras no se aprobase la Ley General en Materia de Datos Personales en Posesión de Sujetos Obligados, dicha normativa local permanecería vigente.

Modernizar la legislación local debe ser una obligación inherente al legislador zacatecano; por ello, avanzar en materia de protección de datos personales en posesión de sujetos obligados significa reconocer desde el ámbito de la ley que todos los datos personales de personas físicas y morales son de alta relevancia para el Estado; significa reconocer como derecho humano, la protección de la información más importante para toda persona física y moral; significa un compromiso entre el Estado y la sociedad en la implementación de una cultura y educación respecto al uso de los datos personales desde el sector público; significa generar una nueva visión en los servidores públicos sobre el tratamiento de información sensible de las personas y sobre todo; significa dignificar a las personas en el reconocimiento del derecho que todas y todos tenemos como personas físicas y morales para primero, conocer el o los responsables del manejo y tratamiento de nuestros datos personales y segundo, del derecho que todos tenemos al acceso, rectificación, cancelación u oposición del uso de nuestros datos personales.

Valdría la pena precisar que esta normativa que se presenta para el Estado de Zacatecas, referente a la protección de datos personales en posesión de sujetos obligados, por sí misma, constituye y define una limitante a la normativa que otorga el derecho al acceso a la información. Sin embargo, ambas lejos de ser excluyentes, son complementarias ya que el acceso a la información debe también contemplar el derecho a la privacidad de los datos personales de cualquier persona física o moral.

Son dos realidades las que día a día generan la necesidad apremiante de instituir controles de protección de datos personales. La primera es sin duda el gran avance tecnológico que ha facilitado de una manera excepcional la captura y la trasmisión de información. Hoy se vive en un mundo conectado por la tecnología a través de flujos enormes de datos e información. Tan sólo en 2016, según la Organización para la Cooperación del Desarrollo Económico, en México 50 de cada 100 habitantes se encuentran conectados a internet ya sea por modem fijos, teléfono celular, en domicilios particulares, negocios, espacios públicos o dependencias de gobierno[5].

La segunda realidad, la encontramos en la cotidianidad de cualquier personas cuando asiste alguna dependencia pública en busca de un servicio público, cuando

[5] http://www.oecd.org/sti/broadband/broadband-statistics-update.htm (Fecha de consulta 3 de febrero de 2017)

la persona acude a cumplir con sus obligaciones tributarias, cuando le asiste una necesidad de salud, cuando acude a la autoridad en busca de procuración de justicia, en fin, cuando toda persona ejerce sus derechos y busca un servicio o bien público. Estas dos realidades descritas confabulan un universo de información al que si bien, cualquiera tiene derecho a conocer, también genera un alto riesgo de que dicha información no se trate adecuadamente y genere casos de arbitrariedad y abuso sobre el tratamiento de la información afectando así la dignidad de las personas.

Cabe resaltar, que el derecho que ésta ley propone respecto a la protección de datos personales en posesión de sujetos obligados se limitará sólo por causas de seguridad nacional, disposiciones de orden público, seguridad, salud pública o para salvaguardar derechos de terceros, tal como lo hace la Ley General en la materia. Igualmente, esta ley que se promueve define el concepto de datos sensibles como aquella información más íntima del titular y cuyo mal manejo pueda generar discriminación racial, étnica, religiosa, filosófica, moral, sexual o de salud. Dichos datos sensibles se amparan en la Declaración Universal de Derechos Humanos que en su artículo 12 dice:

"*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia… Toda persona tiene derecho a la protección de la ley contra tales injerencias…*"[6].

Finalmente, esta ley define sanciones a los sujetos obligados que hagan mal uso, divulguen, oculten, alteren, mutilen, destruyan, inutilicen, total o parcialmente los datos personales de cualquier persona física o moral.

No obstante, esta ley mantiene un espíritu normativo el cual pretende además de proteger los datos más íntimos de las personas, busca concientizar y educar tanto a las instituciones públicas, sus servidores públicos y a las personas. En el ámbito público esta ley pretende profesionalizar y modernizar el quehacer público en el ámbito el tratamiento de la información, y en lo que le toca a las personas se busca generar una conciencia –autodeterminación– sobre el derecho a conocer y entender el manejo sobre sus datos personales.

CUARTO. En sesión ordinaria del 6 de abril de 2017, se dio lectura a la iniciativa con proyecto de decreto por el que se expide la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Zacatecas, que presentó el diputado Jorge Torres Mercado, en ejercicio de las facultades que le confieren los artículos 60 fracción I de la Constitución Política del Estado de Zacatecas; 46 fracción I y 48 fracción II de la Ley Orgánica del Poder Legislativo del Estado y 95 fracción I de su Reglamento General.

---

[6] Declaración Universal de los Derechos Humanos de 1948. Artículo 12.

QUINTO. En esa misma fecha, por acuerdo de la Presidencia de la Mesa Directiva, la iniciativa referida fue turnada mediante memorándum número 0603 a esta Comisión Legislativa para su estudio y dictamen correspondiente.

SEXTO. El proponente justificó su iniciativa en la siguiente

EXPOSICIÓN DE MOTIVOS

Los avances tecnológicos han venido a revolucionar el manejo de la información, de manera particular podemos decir que los datos personales se han convertido en un activo para las empresas, según datos del Banco Mundial el uso de internet a nivel internacional para el año 2015 se situó en 44 por cada 100, es decir que el 44% de la población mundial hace uso de la red, si nos situamos en América del Norte este número se incrementa de manera significativa a 75,9. En nuestro país representa el 57.4% lo que nos sitúa por encima de la media mundial.

Sin embargo, los antecedentes en cuanto a reglamentación del uso y manejo de datos personales es relativamente reciente, el artículo 12 de la Declaración Universal de los Derechos Humanos, del 10 de diciembre de 1948, señala ya la prohibición de injerencias arbitrarias en la vida privada, familiar, domicilio o correspondencia.

El Convenio para la Protección de los Derechos Humanos y Libertades y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, establecen ambas en su artículo 8 el derecho al respeto de la vida privada y familiar, de su domicilio y correspondencia.

El Pacto Internacional de Derechos Civiles y Políticos, así como la Convención Americana sobre Derechos Humanos de 1966 y 1969, establecen ya como un derecho la protección de la vida privada, familiar, de su domicilio o correspondencia ni de ataques ilegales a su honra o reputación.

El desarrollo tecnológico y el incremento en los flujos de información a nivel internacional no tiene fronteras, el intercambio de información con datos personales a través de las redes electrónicas ha llevado a la comunidad internacional a emitir una serie de regulaciones que tienen como objetivo proteger la información personal en el área de la transferencia de datos a nivel internacional. Según datos del Banco Mundial, en 2015 México contaba con un promedio de 39 servidores seguros por cada millón de personas, muy por debajo de la media mundial que es de 209, si nos situamos en América del Norte este panorama es aún más desalentador, ya que el

promedio para esta zona geográfica es de 1,617 servidores seguros por millón de personas.

Ante estos datos resulta inaplazable la configuración de un marco jurídico que regule el adecuado tratamiento de los datos personales, especialmente los que se encuentran en poder del Estado, ya que como podemos apreciar no existe actividad económica que para el desarrollo de la misma quede dispensada de la interacción, explotación, aprovechamiento y transferencia de información personal.

La importancia de la protección de datos personales en un contexto mundial que al menos en la Red ha desdibujado sus fronteras resulta inaplazable, la regulación de todas y cada una de las tecnologías que manejan información personal deben ser previstas y sancionadas a fin de salvaguardar la información que se ha convertido en un activo fundamental y necesario para el desarrollo y crecimiento de todas las economías nacionales.

En el plano nacional, el primer registro mediante el cual se reconoce al derecho de protección de los datos personales en nuestro país, data de la reforma por la que se modificó el contenido del artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, en el año del 2007. Dicha reforma reconoce al acceso a la información como una garantía fundamental de todo individuo.

Dentro de los agregados al mencionado artículo, se encuentra las fracciones II y III, apartados que se constituyeron como primeras regulaciones en materia de protección de datos personales. Dichas fracciones se establecieron como limitantes al ejercicio del derecho de acceso a la información, al enunciar literalmente lo siguiente:

“II. La información a que se refiere la vida privada será protegida en términos de ley respectiva.

III. Toda persona tiene derecho a acceder y rectificar sus datos personales.”

Para el año del 2009, se logra consolidar la figura de “protección de datos personales”. Se aprueban reformas a los artículos 16 y 73 de nuestra Carta Magna.

El artículo 16 párrafo segundo, incorpora al listado de garantías individuales, el derecho a la protección de datos personales. La descripción literal del párrafo segundo se detalla de la siguiente manera:

“Artículo 16…

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los

principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

Por su parte, el artículo 73 Constitucional, otorga la faculta irrestricta al Congreso de la Unión, para legislar en materia de protección de datos personales en posesión de particulares.

La Ley que en un primer momento regulo aspectos de la vida privada, fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Algunas características de la Ley aludida, son los siguientes:

- Se reconoce por primera vez en México la protección de los datos personales.

- Se limita a las bases de datos del sector público a nivel federal. Es a la vez, una ley de acceso a la información y una ley de protección de datos personales (limitada en su ámbito de aplicación).

- Su capítulo IV establece un marco muy general que regula la obtención, almacenamiento, transmisión, uso y manejo de los datos personales en posesión de dependencias y entidades federales.

En el año del 2010 se promulga la Ley Federal de Protección de Datos Personales en posesión de los particulares, como primera norma reglamentaria de lo que dispone los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.

El mencionado ordenamiento tiene como principal objetivo, la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

En febrero de 2014, el artículo 6 de la Constitución Política de los Estado Unidos Mexicanos, sufre una nueva modificación en materia de protección de datos personales. Se agregó una fracción VIII al mencionado artículo, donde se pueden observar las siguientes características:

- Se transforma la naturaleza jurídica del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, así como la de sus homólogos en los Estados de la República. En todos los casos se establece condición de Órganos Constitucionales Autónomos especializados, responsables de garantizar la protección de los datos personales.

- Con la nueva naturaleza autónoma de los Órganos Garantes del derecho a la protección de datos personales, se establece la posibilidad de que sus miembros sean sometidos a juicio político.

- Se amplía el abanico de Sujetos Obligados por la legislación, en materia de transparencia y acceso a la información pública, siendo aplicable también a los responsables de la protección de datos personales.

- Se expresa la obligación por parte de la Federación y los Estados, para establecer procedimientos de revisión expeditos, en materia de protección de datos personales, que se sustanciarán ante los Organismos Autónomos especializados e imparciales.

- Se faculta al Órgano Constitucional Autónomo de carácter nacional, para conocer de los recursos que interpongan los particulares respecto de las resoluciones emitidas por los Organismo Especializados Autónomos de los Estados, que determinen la reserva, confidencialidad, inexistencia o negativa en materia de datos personales.

  En el mismo artículo 6º apartado A, inciso VIII de nuestra Carta Fundamental, se precisó que el Congreso de la Unión, debería emitir una Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, con el fin de establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

  En estricto acatamiento a lo antes señalado, en diciembre del 2016, el Congreso de la Unión aprobó el contenido de la Ley General en materia de protección de datos personales, misma que fue enviada al Poder Ejecutivo Federal para su promulgación. Siendo así lo anterior, el día 26 de enero del 2017, se publicó le referido ordenamiento en el Diario Oficial de la Federación.

  Los aspectos fundamentales de la Ley, los podemos resumir en los siguientes puntos:

- En el ámbito de aplicación de esta norma se encuentran los sujetos obligados descritos en el párrafos 5to y 6to del artículo 1ro, dentro de los cuales destacan los sindicatos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física o moral que reciba y ejerza recursos públicos o realicen actos de autoridad en ámbito federal, estatal y municipal.

- El Sistema Nacional de Transparencia, será la instancia encargada de coordinar y evaluar las acciones relativas a la política pública transversal de protección de datos personales, así como implementar criterio y lineamientos en la materia.

- Son derechos inalienables de todas las personas acceder, rectificar, cancelar y oponerse a sus datos personales.

- Toda transferencia de datos personales, se encuentra sujeta al consentimiento de su titular.

- El comité de transparencia de cada Sujeto Obligado, será la autoridad máxima en materia de protección de datos personales.

- Se garantizan dos medios de impugnación; recurso de revisión y el recurso de inconformidad. Respecto al recurso de revisión se faculta al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para atraer aquellos recursos que por su interés y trascendencia así lo ameriten.

- Se prevén medidas de apremio y sanciones para los funcionarios públicos que infrinjan alguna de las disposiciones de la multicitada ley.

Un aspecto esencial del ordenamiento, radica en lo que dispone el artículo segundo de los transitorios el cual menciona lo siguiente:

"Segundo. La Ley Federal de Transparencia y Acceso .a la Información Pública, las demás leyes federales y las leyes vigentes de las Entidades Federativas en materia de protección de datos personales, deberán ajustarse a las disposiciones previstas en esta norma en un plazo de seis meses siguientes contado a partir de la entrada en vigor de la presente Ley."

Resulta inherente a todo individuo la necesidad de proteger su esfera más íntima. Una vida privada vulnerable a injerencias no permitidas, se traduce en una importante limitación para el desarrollo común de las personas, por tanto, resulta inconcusa la necesidad de todo sujeto a la vida privada. En consecuencia, el derecho de todo ciudadano a proteger su probidad, debe de ser reconocido y tutelado por el Estado, al cual, le corresponde constituir el andamiaje legal, que proteja, garantice y resguarde la esfera más íntima de cualquier ciudadano.

MATERIA DE LAS INICIATIVAS. Expedir la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Zacatecas.

Con fundamento en el artículo 56 de nuestra Ley Orgánica, los integrantes de esta Comisión consideramos pertinente acumular las iniciativas que se han referido, toda vez que ambas proponen la emisión del mismo ordenamiento legal y las disposiciones que conforman ambas propuestas son similares.

VALORACIÓN DE LA INICIATIVA

Esta Comisión estima adecuado sujetar el presente dictamen a los siguientes

C O N S I D E R A N D O S :

PRIMERO. COMPETENCIA. Esta Comisión Legislativa es competente para estudiar y analizar las iniciativas en referencia, presentadas ante esta Soberanía Popular, así como para emitir el dictamen correspondiente, de conformidad con lo previsto en los artículos 123, 124, fracción XVII, 125, fracción I, y 144, de la Ley Orgánica del Poder Legislativo del Estado de Zacatecas.

SEGUNDO. ANTECEDENTES. Como se precisa en ambas iniciativas, los artículo 6.° y 16 de nuestra Carta Magna son el sustento constitucional de los derechos humanos de acceso a la información y de protección de datos personales.

En el caso del artículo 6.°, su evolución legislativa ha sido, por decirlo de alguna forma, lenta pero consistente, pues solo ha sido objeto de seis reformas: la primera de ellas en 1977, es decir, 60 años después de la promulgación de nuestro texto fundamental; la segunda reforma se llevó a cabo en 2007, treinta años después de la primera.

Entre una y otra, los avances son enormes y significativos: tan solo en el aspecto cuantitativo, de 45 palabras pasa a 257, distribuidas en un párrafo adicional y siete fracciones.

En el aspecto cualitativo, los avances son notables: se precisa el contenido de ambos derechos fundamentales –acceso a la información pública y protección de datos personales–; se crea un organismo dotado de autonomía técnica responsable de garantizar el goce y disfrute de tales derechos y se establece el principio de máxima publicidad como criterio fundamental de interpretación en la materia.

Las subsecuentes reformas han fortalecido y consolidado la cultura de la transparencia y la rendición de cuentas; en la reforma constitucional más reciente, del 29 de enero de 2016, se ha otorgado autonomía plena a los organismos garantes –federal y locales–, y se han establecido razones de interés público y seguridad nacional como únicas excepciones al principio de máxima publicidad.

Por lo que se refiere al artículo 16 constitucional, en dicho numeral se establece el derecho humano de legalidad, consistente en que nadie podrá ser molestado en su persona, bienes o familia, sino mediante mandato escrito de autoridad competente.

Lo mismo que el artículo 6.°, el referido numeral ha sido objeto de seis reformas, la primera en 1983; fue hasta el año de 2009 cuando se adicionó un segundo párrafo

al citado artículo 16 para incorporar la protección de datos como un derecho fundamental:

Artículo 16. …

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

Ambas disposiciones constitucionales son el sustento del derecho fundamental a la protección de datos personales y conforme a ellos se estructuran la Ley General y las iniciativas que hoy se dictaminan.

Como lo hemos visto, los avances en nuestro marco constitucional se han dado en un espacio de nueve años, 2007-2016 y, sin duda, podemos afirmar que nuestra Carta Magna cuenta con disposiciones de vanguardia que han permitido el ejercicio pleno de los derechos fundamentales que hemos mencionado.

En tal contexto, las iniciativas que se estudian tienen como objetivo complementar el Sistema de Transparencia y Acceso a la Información Pública previsto en la Constitución Federal, toda vez que es necesario regular, y proteger, la información de los particulares en posesión de los sujetos obligados.

TERCERO. LA PROTECCIÓN DE DATOS Y EL DERECHO A LA INTIMIDAD. La libertad personal es un derecho de primera generación, muy particularmente, el reconocimiento del derecho a la intimidad de la persona como una prerrogativa objeto de tutela por parte del Estado.

Citando a Bidart Campos, Miguel Carbonell expresa, en torno a los derechos de primera generación, lo siguiente:

a) Derechos de la primera generación. Los identifica con los derechos civiles y políticos clásicos originados en el constitucionalismo moderno: derecho a la vida, a la integridad, a la libertad, a la igualdad, a la participación política, a la seguridad, etcétera. Tienen su raigambre en la *Declaración de derechos* de 1789.[7]

En tal contexto, los avances tecnológicos han venido a revolucionar el manejo de la información y la perspectiva, precisamente, de los derechos de primera generación;

[7] http://www.miguelcarbonell.com/artman/uploads/1/Cat_logo_de_Derechos_Fundamentales.pdf

en ese sentido, los datos personales se han convertido en un activo, pues el uso de internet para el año 2015, según datos del Banco Mundial, se situó en 44 por cada 100; en México, esta proporción se eleva hasta el 57.4%.

El desarrollo tecnológico ha redimensionado las relaciones del hombre, podemos afirmar que los sistemas tecnológicos de transmisión de datos se han convertido en el símbolo emblemático de la cultura contemporánea.

Sin duda, el uso de las herramientas tecnológicas ha facilitado el procesamiento de datos e información proporcionada por los usuarios de los servicios prestados por los entes públicos y privados; como lo afirma Isabel Davara F. de Marcos

Cada vez más significativamente, en número y en calidad, la persona ve cómo su información personal es tratada y evaluada en relación con un sinfín de actividades diversas: buscar empleo, solicitar un crédito, asistir a un centro educativo, realizar la compra semanal, son tan sólo ejemplos de la multitud de situaciones en las que la información personal se ve comprometida.[8]

De acuerdo con lo anterior, el fácil acceso a la información generada por los sujetos obligados, puede propiciar un uso inadecuado de los datos proporcionados por los particulares al solicitar algún servicio; virtud a ello, la necesidad de establecer reglas claras y precisas que regulen el tratamiento que se da a tal información.

Con base en lo expresado, debemos señalar que la protección de datos implica proteger el derecho a la vida privada y a la intimidad de las personas, en tal virtud, solo a ellas debe corresponder el derecho a "decidir quién, cómo, dónde, cuándo y para qué se tratan sus datos personales"[9], en ese sentido, consideramos que ambas iniciativas establecen las bases para garantizar ese derecho fundamental.

Es decir, las leyes deben establecer un equilibrio entre el derecho a la información y la autodeterminación informativa, como un derecho inalienable e intransferible de los individuos, virtud a ello, la necesidad de contar con ordenamientos legales actuales y modernos que provean de las herramientas suficientes para la protección de los datos de los particulares en posesión de entes públicos o privados.

Virtud a ello, el derecho a la intimidad, consagrado en el artículo 12 de la Declaración Universal de los Derechos Humanos (1948), señala la prohibición de injerencias arbitrarias en la vida privada, familiar, domicilio o correspondencia, se ha visto en la necesidad de evolucionar para resguardar la privacidad en sus nuevos matices.

---

[8] http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf

[9] Ibidem

Esta Comisión dictaminadora coincide en que los datos personales se han convertido en una práctica habitual de control y almacenamiento por parte del sector público –y privado–, virtud a ello, concuerda en la necesidad de redimensionar el espectro de protección del derecho a la intimidad, es decir, que además de la facultad del individuo de rechazar invasiones a su ámbito privado, ahora supone el reconocimiento de un derecho de control y acceso a su información.

El uso y control sobre los datos personales debe ser reconocido ya no sólo como una mera prerrogativa, sino además como un derecho fundamental protegido y garantizado a través de mecanismos de protección eficientes.

En ese marco, el derecho a la intimidad engloba todo aquello que se considera más propio y oculto del ser humano; la intimidad, anteriormente, era la facultad destinada a salvaguardar un determinado espacio con carácter exclusivo y consistía, básicamente, en el derecho del individuo a la soledad.

Al igual que el resto de los derechos humanos, el derecho a la intimidad ha evolucionado y, como tal, ha sido reconocido por las normas jurídicas y puede justificarse por su capacidad de promover ciertos bienes básicos para los ciudadanos, como pueden ser la libertad, la igualdad, la seguridad y otros similares.

Stuart Mill consideraba que los aspectos concernientes al individuo consistían en el derecho a una absoluta independencia, puesto que sobre sí mismo, sobre su cuerpo y mente, el individuo era soberano.[10]

Actualmente, frente a la sociedad de la información, resulta insuficiente concebir a la intimidad como un derecho garantista de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla al mismo tiempo, como un derecho activo de control sobre el flujo de informaciones que afectan a cada sujeto.[11]

En la modernidad, el derecho a la intimidad, como el más reciente derecho individual relativo a la libertad, ha variado intensamente, fruto de la revolución tecnológica. Por ello, esta Comisión dictaminadora coincide con la necesidad de ampliar su ámbito de protección, así como el establecimiento de nuevos instrumentos de tutela jurídica, como las iniciativas que se estudian.

Todo ciudadano registrado en un banco de datos se encuentra expuesto a una vigilancia continua e inadvertida que afecta potencialmente los aspectos más sensibles de su vida privada, por su variedad y multiplicidad, y hoy, además de

[10] Stuart Mill, John, *Sobre la libertad,* 6a. ed., trad. de Pablo de Azcárate, Madrid, Alianza Editorial, 2004.
[11] Pérez Luño, A. E., Derechos humanos, Estado de derecho y Constitución, 9a.ed., Madrid, Tecnos, pp. 336.

tomar conciencia de ello, comienza a exigir un reconocimiento sobre el uso y control de sus datos.

Las nuevas tecnologías, al facilitar la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas y de recopilación de datos, se presentan como una exigencia inaplazable de regulación, que no podemos, ni debemos postergar.

Los antecedentes, en cuanto a reglamentación del uso y manejo de datos personales, es relativamente reciente: el artículo 12 de la Declaración Universal de los Derechos Humanos, del 10 de diciembre de 1948, señala lo siguiente:

Artículo 12.
Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Dicha enunciación, considerada como el derecho a la intimidad en su ámbito estático, se encuentra reconocida en la mayoría de las normas constitucionales, sin embargo, el uso generalizado de las nuevas tecnologías nos obliga a darle un nuevo contenido y establecer herramientas jurídicas adecuadas para su protección.

El desarrollo tecnológico y el incremento en los flujos de información a nivel internacional no tiene fronteras, el intercambio de información con datos personales a través de las redes electrónicas ha llevado a la comunidad internacional a emitir una serie de regulaciones que tienen como objetivo proteger la información personal en el área de la transferencia de datos a nivel internacional.

Según datos del Banco Mundial, en 2015 México contaba con un promedio de 39 servidores seguros por cada millón de personas, muy por debajo de la media mundial que es de 209, esta información nos hace ver lo imperativo de regular jurídicamente los usos y abusos en el manejo de datos.

Los datos de todo individuo deben ser objeto de protección para que éstos puedan ser tratados o elaborados y, finalmente, ser convertidos en información, y utilizados, exclusivamente, para los fines autorizados por sus titulares.

Hondius, define la protección de datos en los términos siguientes:

…aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos.[12]

[12] Hondius, F. W., "A Decade of International Data Protection", Netherlands International Law Review, vol. 30, núm, 2, 1983, p. 105

Con base en lo anterior, el concepto evolucionado de intimidad, en la era de la informática, concede derechos a los individuos respecto de sus datos personales que son objeto de tratamiento computarizado, e impone obligaciones y deberes de aquellos que controlan y tienen acceso a esos datos personales, particularmente, los que se encuentran en posesión de los poderes del Estado.

En nuestro país, en 1917, la Constitución Política de los Estados Unidos Mexicanos estableció derechos relativos a la libertad individual, de entre los que destacan la inviolabilidad de correspondencia y domicilio, y más adelante, el secreto a las comunicaciones privadas.

Con la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública, en 2002, se establece la primera aproximación a la protección de datos personales, sin embargo, sólo alude a su uso y destino, por lo que la nueva Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados viene a complementar la inviolabilidad de la información más íntima y delicada de los ciudadanos mexicanos.

Sobre el derecho a la intimidad y a la autodeterminación informativa, los tribunales federales han emitido diversos criterios, entre ellos, el siguiente:

Época: Novena Época. Registro: 168944. Instancia: Tribunales Colegiados de Circuito. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta, Tomo XXVIII, Septiembre de 2008. Materia(s): Civil. Tesis: I.3o.C.695 C. Página: 1253

DERECHO A LA INTIMIDAD. SU OBJETO Y RELACIÓN CON EL DERECHO DE LA AUTODETERMINACIÓN DE LA INFORMACIÓN. Los textos constitucionales y los tratados internacionales de derechos humanos recogen el derecho a la intimidad como una manifestación concreta de la separación entre el ámbito privado y el público. Así, el derecho a la intimidad se asocia con la existencia de un ámbito privado que se encuentra reservado frente a la acción y conocimiento de los demás y tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sea simples particulares o bien los Poderes del Estado; tal derecho atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia; asimismo garantiza el derecho a poseer la intimidad a efecto de disponer del control sobre la publicidad de la información tanto de la persona como de su familia; lo que se traduce en el derecho de la autodeterminación de la información que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede

utilizar esa información. En este contexto, el derecho a la intimidad impone a los poderes públicos, como a los particulares, diversas obligaciones, a saber: no difundir información de carácter personal entre los que se encuentran los datos personales, confidenciales, el secreto bancario e industrial y en general en no entrometerse en la vida privada de las personas; asimismo, el Estado a través de sus órganos debe adoptar todas las medidas tendentes a hacer efectiva la protección de este derecho.

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.

Amparo en revisión 73/2008. 6 de mayo de 2008. Mayoría de votos. Disidente: Neófito López Ramos. Ponente: Víctor Francisco Mota Cienfuegos. Secretario: Erick Fernando Cano Figueroa.

En tal contexto, debemos expresar que el primer antecedente internacional para la protección de datos fue el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, instrumento donde se precisan, ya, los principios y criterios aplicables en la materia, por ejemplo, en su artículo 5 se establece lo siguiente:

Artículo 5. Calidad de los datos

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente;

b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) serán exactos y si fuera necesario puestos al día;

e) se conservarán bajo una forma que permita la identificación de las personas interesadas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

El avance de las tecnologías de la información nos obliga, como legisladores, a establecer las herramientas para que los particulares puedan proteger los datos que aportan, en este caso, a los entes públicos.

En ese sentido, esta Comisión de dictamen considera que ambas iniciativas cumplen con tal objetivo, pues en ellas se precisan las obligaciones en la materia a

cargo de los sujetos obligados y procedimientos específicos para el resguardo y tratamiento de los datos de particulares que se encuentran en su poder con motivo del ejercicio de sus funciones.

CUARTO. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, DESDE SU PERSPECTIVA MÁS AMPLIA. En junio de 2011, el Constituyente Permanente reconoció que los derechos humanos son la base y el objeto de las instituciones públicas, así entonces, la parte dogmática de la Constitución es la piedra angular sobre la que se sustenta la legitimidad del estado mexicano.

El artículo 1º de nuestra Constitución Federal, es muy clara y puntual al establecer lo siguiente:

Artículo 1o. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.

A partir de la citada reforma constitucional, debemos contemplar el derecho a la protección de los datos personales, desde una perspectiva más amplia, toda vez que los efectos de la referida modificación, impactan directamente en la labor de las autoridades del país, ya que deben hacer efectivos los derechos humanos reconocidos tanto en la Constitución Federal como en los tratados internacionales de los que el Estado mexicano forma parte.

La protección de datos personales no debe verse en forma aislada, pues se trata de un aspecto que forma parte de un sistema más amplio integrado por varios elementos:

- Transparencia.
- Acceso a la Información.
- Rendición de cuentas.
- Protección de datos personales.
- Derecho de réplica y libertad de expresión
- Organización y administración homogénea de archivos.

De acuerdo con los tribunales federales, el sistema referido está integrado por los siguientes preceptos constitucionales:

Época: Décima Época. Registro: 2013674. Instancia: Tribunales Colegiados de Circuito. Tipo de Tesis: Aislada. Fuente: Gaceta del Semanario Judicial de la

Federación, Libro 39, Febrero de 2017, Tomo III. Materia(s): Constitucional. Tesis: I.2o.A.E.1 CS (10a.) Página: 2364

SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES Y DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. PRECEPTOS CONSTITUCIONALES QUE LOS REGULAN. Si bien es cierto que el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos establece los principios, directrices y reglas básicas sobre las cuales se construyen los sistemas de protección de datos personales y de transparencia y acceso a la información pública, también lo es que en el propio Texto Constitucional se contienen otras reglas específicas al respecto, como ocurre tratándose de la identidad y de los datos personales de las víctimas y ofendidos partes en el procedimiento penal (artículo 20, apartado C, fracción V), del régimen de telecomunicaciones (artículos tercero y octavo transitorios del decreto de reforma en la materia, publicado en el Diario Oficial de la Federación el 11 de junio de 2013), la fiscalización de recursos públicos ejercidos por personas privadas (artículo 79), la creación del Sistema Nacional de Información Estadística y Geográfica (artículo 26, apartado B), el registro público sobre deuda pública (artículo 73, fracción VIII, inciso 3o.), la investigación y sanción de responsabilidades administrativas y hechos de corrupción, tratándose de información fiscal o relacionada con el manejo de recursos monetarios (artículo 109, fracción IV), el Sistema de Información y Gestión Educativa (artículo quinto transitorio del decreto de reformas publicado en el señalado medio el 26 de febrero de 2013), la recopilación de información geológica y operativa a cargo de la Comisión Nacional de Hidrocarburos [artículo décimo transitorio, inciso b), del decreto de reformas constitucionales difundido el 20 de diciembre de 2013], el sistema de fiscalización sobre el origen y destino de los recursos de los partidos políticos, coaliciones y candidatos (artículo segundo transitorio del decreto de reformas publicado el 10 de febrero de 2014) y la fiscalización de la deuda pública (artículo séptimo transitorio del decreto que modifica diversas disposiciones constitucionales, publicado el 26 de mayo de 2015).

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA ESPECIALIZADO EN COMPETENCIA ECONÓMICA, RADIODIFUSIÓN Y TELECOMUNICACIONES, CON RESIDENCIA EN LA CIUDAD DE MÉXICO Y JURISDICCIÓN EN TODA LA REPÚBLICA.

Amparo en revisión 165/2015. Teléfonos de México, S.A.B. de C.V. 26 de agosto de 2016. Unanimidad de votos. Ponente: Adriana Leticia Campuzano Gallegos. Secretario: Arturo Mora Ruiz.

Amparo en revisión 164/2015. Teléfonos del Noroeste, S.A. de C.V. 23 de septiembre de 2016. Unanimidad de votos. Ponente: Arturo Iturbe Rivas. Secretaria: Laura Zárate Muñoz.

Esta tesis se publicó el viernes 10 de febrero de 2017 a las 10:12 horas en el Semanario Judicial de la Federación.

En tal contexto, resulta incuestionable que el análisis de las iniciativas de Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados, tienen como sustento la reforma constitucional en materia de derechos humanos, por lo que resulta indispensable estudiar, desde una perspectiva más amplia, el derecho que posee todo individuo a la protección de sus datos personales.

QUINTO. MODIFICACIONES A LAS INICIATIVAS. Esta Comisión Legislativa, después de haber estudiado y analizado en detalle ambas iniciativas, estima pertinente efectuar las modificaciones siguientes, con el fin de lograr una cabal armonización del contenido de nuestra ley estatal con las disposiciones y principios de la Ley General en la materia:

1. Participación Ciudadana. Para esta Comisión dictaminadora es importante referir el ejercicio de Gobierno Abierto que se llevó a cabo el pasado jueves 11 de mayo del año en curso, donde esta Comisión de dictamen, por conducto de su Presidente, el Diputado Jorge Torres Mercado, organizó un evento cuyo principal objetivo fue involucrar a la sociedad en general, en la conformación de una Ley en materia de datos personales, adaptada a las necesidades de la sociedad zacatecana.

En el citado evento participó el licenciado José Luis Galarza Esparza, Director de Inspección en la Dirección General de Investigación y Verificación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), quien planteó la necesidad de contar con leyes estatales armonizadas con la general y, sobre todo, con normas jurídicas modernas y actuales que permitan garantizar la protección de datos personales.

De la misma forma, fueron valiosas las aportaciones del público, integrado por personas interesadas en el tema y que formularon diversas propuestas, entre ellas, hicieron especial énfasis en el denominado derecho al olvido.

Las condiciones actuales en las que se desenvuelven las sociedades, trae como consecuencia el surgimiento de nuevas preocupaciones por parte de los ciudadanos; la eliminación o bloqueo de datos en internet y en buscadores web, la cancelación de antecedentes penales, la salida de ficheros de morosos y de listados comerciales, así como el mal uso de la información de las personas fallecidas, son algunas acciones que menoscaban los derechos fundamentales de los individuos, por ello, con el llamado derecho al olvido, se busca garantizar el honor y la intimidad

de una persona desligándola de acontecimientos que la afecten de manera negativa.

Referido lo anterior, debemos señalar que en la Unión Europea es donde se ha desarrollado de manera más consistente el derecho al olvido y con base en diversos tratados vigentes en ella, esta Comisión puede definirlo de la forma siguiente:

El derecho que tiene el titular de un dato personal para que le sea borrada, bloqueada o suprimida información de carácter personal, ya que de no hacerlo se pudiera afectar, de alguna manera, el libre desarrollo de sus derechos fundamentales.

La evolución del derecho al olvido, en el contexto internacional, tiene como principal sustento, como hemos visto, los convenios vigentes en Europa. Después de la Segunda Guerra Mundial, los sistemas jurídicos de aquel continente, mostraron una evolución centrada en la revaloración de los derechos de la personalidad como elementos fundamentales de su ordenamiento jurídico.

Lo anterior obligó a entender las disposiciones legales de un modo más amplio, así como a considerar y equilibrar intereses contrapuestos, que en el caso que nos ocupa, por un lado, involucra al derecho del individuo a vivir sin injerencias injustificadas que vulneren sus derechos, su autonomía y sus posibilidades de desarrollo y, por otro, la libertad de expresión e información, entendida como un elemento fundamental en la sociedad democrática.

En tal sentido, la Unión Europea promulgó en el año del 2016, el denominado Reglamento General de Protección de Datos, cuerpo legal que reconoce por primera ocasión al derecho al olvido como una garantía fundamental de los individuos. La citada norma establece en su artículo 17 lo siguiente:

Artículo 17

Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.[13]

   En México no existe, como tal, una norma que regule propiamente al derecho al olvido, pero existen antecedentes importantes; el primer registro lo encontramos en el proceso legislativo de reformas a la Ley para Regular las Sociedades de Información Crediticia, en el que se señaló

   …pasando 7 años de un pago parcial o una mensualidad, este será borrado obligatoriamente del historial crediticio de una persona; así, se eliminarán de la base de datos los registros con la información de personas físicas y morales sobre créditos vencidos…

   Los tribunales federales han emitido criterios que, si bien no son exclusivos del concepto del derecho al olvido, tocan aspectos relativos a esta garantía:

   Época: Décima Época. Registro: 2011407. Instancia: Tribunales Colegiados de Circuito. Tipo de Tesis: Jurisprudencia. Fuente: Gaceta del Semanario Judicial de la Federación, Libro 29, Abril de 2016, Tomo III. Materia(s): Común. Tesis: XX.1o.P.C. J/1 (10a.) Página: 2045

[13] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.SPA&toc=OJ:L:2016:119:TOC

FICHA SIGNALÉTICA. SI SE OTORGÓ AL SENTENCIADO EL AMPARO Y EN CUMPLIMIENTO A LA EJECUTORIA CORRESPONDIENTE, LA AUTORIDAD RESPONSABLE TIENE QUE EMITIR SENTENCIA ABSOLUTORIA A SU FAVOR, DE OFICIO Y SIN MAYOR TRÁMITE, DEBE ORDENAR LA CANCELACIÓN Y DESTRUCCIÓN DE AQUÉLLA (INTERPRETACIÓN EXTENSIVA Y SISTEMÁTICA DEL ARTÍCULO 304, PÁRRAFOS PRIMERO Y ÚLTIMO, DEL CÓDIGO DE PROCEDIMIENTOS PENALES PARA EL ESTADO DE CHIAPAS ABROGADO, EN RELACIÓN CON EL DIVERSO 77, FRACCIÓN I, DE LA LEY DE AMPARO). Si bien es cierto que el Código de Procedimientos Penales para el Estado de Chiapas (abrogado) no contempla disposición expresa, en el sentido de que cuando el procesado obtenga sentencia absolutoria debe ordenarse la cancelación de su ficha signalética, también lo es que del artículo 304, párrafos primero y último, del mismo ordenamiento se advierte que el legislador local estableció el derecho del gobernado a solicitar la cancelación de sus antecedentes penales, cuando justifique, con copias certificadas, la existencia de autos de sobreseimiento, sentencias absolutorias o cualquier otra resolución que implique la ausencia de responsabilidad penal; por tanto, de una interpretación extensiva y sistemática de esas porciones normativas, en relación con el artículo 77, fracción I, de la Ley de Amparo, se concluye que cuando se otorgue el amparo y la protección de la Justicia Federal al sentenciado y en cumplimiento a la ejecutoria correspondiente, la autoridad responsable tenga que emitir una sentencia absolutoria a su favor, de oficio y sin mayor trámite, debe ordenar la cancelación y destrucción del registro de identificación administrativa, con el objeto de restituirlo en el pleno goce de sus derechos vulnerados, a fin de restablecer las cosas al estado que guardaban antes de dicha violación.

PRIMER TRIBUNAL COLEGIADO EN MATERIAS PENAL Y CIVIL DEL VIGÉSIMO CIRCUITO.

Amparo directo 4/2015. 10 de diciembre de 2015. Unanimidad de votos. Ponente: Carlos Arteaga Álvarez. Secretario: José Martín Lázaro Vázquez.

Amparo directo 111/2015. 22 de enero de 2016. Unanimidad de votos. Ponente: Carlos Arteaga Álvarez. Secretaria: Marylin Ramírez Avendaño.

Amparo directo 142/2015. 12 de febrero de 2016. Unanimidad de votos. Ponente: Carlos Arteaga Álvarez. Secretario: Álvaro Mauricio Zenteno Chacón.

Amparo directo 46/2015. 26 de febrero de 2016. Unanimidad de votos. Ponente: Jorge Mason Cal y Mayor. Secretario: Ángel Bustillo Gutiérrez.

Amparo directo 219/2015. 14 de marzo de 2016. Unanimidad de votos. Ponente: Jorge Mason Cal y Mayor. Secretario: Salomón Zenteno Urbina.

Nota: Esta tesis es objeto de la denuncia relativa a la contradicción de tesis 181/2016, pendiente de resolverse por la Primera Sala.

Esta tesis se publicó el viernes 8 de abril de 2016 a las 10:08 horas en el Semanario Judicial de la Federación y, por ende, se considera de aplicación obligatoria a partir del lunes 11 de abril de 2016, para los efectos previstos en el punto séptimo del Acuerdo General Plenario 19/2013.

Época: Décima Época. Registro: 2000360. Instancia: Tribunales Colegiados de Circuito. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta, Libro VI, Marzo de 2012, Tomo 2. Materia(s): Constitucional. Tesis: I.6o.P.6 P (10a.) Página: 1140

FICHA SIGNALÉTICA Y ANTECEDENTES PENALES. CONFORME AL PRINCIPIO DE RETROACTIVIDAD EN BENEFICIO DEL REO PROCEDE SU DESTRUCCIÓN SI LA PORCIÓN NORMATIVA QUE PREVEÍA EL TIPO PENAL POR EL QUE SE CONDENÓ AL SENTENCIADO FUE DEROGADA. La garantía constitucional de retroactividad de la ley penal en beneficio del reo, por regla general, no opera cuando existe cosa juzgada, esto es, cuando ya hay sentencia ejecutoriada, incluso, cuando la pena impuesta ya se ejecutó o se declaró prescrita, esto es así, porque de conformidad con el artículo 80 de la Ley de Amparo, el juicio constitucional condiciona su procedencia a la posibilidad de que la sentencia que se dicte produzca la restitución al agraviado en el pleno goce de la garantía individual violada, volviendo las cosas al estado en que se encontraban antes de la conculcación, lo que no se cumpliría cuando existe sentencia ejecutoriada en la que se declaró la plena responsabilidad y se extinguió la pena impuesta. Sin embargo, esta garantía tiene un ámbito de protección más allá de la aplicación del derecho penal sustantivo (demostración del delito y ejecución de la pena), esto es, también opera respecto de las consecuencias jurídicas derivadas del proceso penal que inciden en la esfera de derechos del gobernado, las cuales no pueden quedar incólumes. En este sentido, si la porción normativa que preveía el tipo penal por el que se condenó al sentenciado fue derogada, dejó de ser relevante para el derecho penal y para la potestad punitiva del Estado, lo que beneficia a quienes fueron sentenciados y se les tuvo por extinguida la pena impuesta, aun al existir cosa juzgada; por ende, procede la destrucción de la ficha signalética y de los antecedentes penales derivados del proceso en virtud de que al no existir como delito la conducta, sus consecuencias deben correr la misma suerte; máxime que no se trata de una “simple medida administrativa”, ya que si bien no es una pena técnicamente hablando, ni participa de las características de ser pena infamante y trascendental, lo cierto es que en nuestro medio social y cultural se les considera un medio informativo de la conducta ilícita del inculpado que trasciende a su esfera jurídica, pues el conocimiento de su contenido por los ciudadanos, produce el mismo

impacto que una pena privativa de derechos, ya que tienen un efecto estigmatizante, dado que quien es identificado queda inhabilitado, de hecho, para cargos privados y se convierte en un ciudadano de segundo orden, pues se ataca en forma directa su honra y fama, cuya secuela trasciende, negativamente, en su esfera jurídica.

SEXTO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.

Amparo en revisión 216/2011. 1o. de diciembre de 2011. Unanimidad de votos. Ponente: Roberto Lara Hernández. Secretario: Juan Carlos Salas Juárez.

Con lo anterior, resulta claro que el derecho al olvido, se encuentra en pleno desarrollo, y es un tema que está adquiriendo importancia dentro las agendas comunes de los Poderes Públicos, dadas las nuevas necesidades y garantías que la sociedad demanda para que aspectos importantes de su vida privada, sean resguardados debidamente por el Estado, toda vez que resulta innegable la relación que tiene el derecho al olvido con el derecho de toda persona a la protección de sus datos personales.

Virtud a lo señalado, para los Diputados que integramos esta Comisión de Dictamen, resulta de vital importancia regular dos aristas tocantes al concepto de derecho al olvido, relativas a garantizar los derechos **al honor y la propia imagen,** de las personas fallecidas, y de los individuos que formen parte de un proceso judicial concluido o no, por delitos del fuero común, temas que pueden ser plenamente regulados por la Legislación local en materia de protección de datos personales, ya que se encuentran dentro del ámbito de competencia por el que se rige el Estado de Zacatecas, y con lo que se busca garantizar lo siguiente:

a) Ante el fallecimiento de una persona, consideramos que se debe guardar su honor y dignidad en el sentido más amplio. Conforme a ello, los derechos ARCO se proyectan como un derecho propio de los familiares, toda vez que su memoria constituye una prolongación de dicha personalidad, protegida y asegurada como parte de la honra de la familia. De acuerdo con lo expresado, resulta inalienable el derecho de los familiares, o del representante designado, para determinar qué información desean sustraer del conocimiento de terceros no vinculados con el fallecido.

b) Las personas que son declaradas inocentes dentro de un juicio por falta de elementos para ser procesada, debe contar con todas las garantías de las que gozaba previamente a su proceso judicial. Por tanto, el Estado debe garantizar toda cancelación y, en su caso, la destrucción de cualquier registro que se tenga; toda vez que es un derecho la caducidad del dato negativo, entendido este, como el dato que arroja información que se considera afectaría el desarrollo adecuado de una persona en sociedad.

c) Quienes han vivido la condición de sentenciados a la pérdida de la libertad y transitan hacia la recuperación del goce pleno de sus derechos, buscan que la sociedad los acepte y puedan acceder a otra oportunidad. No obstante, este es un proceso que, en muchos casos conlleva discriminación y exclusión, lo que implica que sean señalados por esta condición. En tal sentido, es necesario considerar que los antecedentes penales, forman parte del pasado de la persona y se encuentran en el ámbito de su vida privada, por tanto, no desea que otros los conozcan por el riesgo a ser discriminado.

En tal sentido, consideramos necesario incluir en el Título tercero relativo "Derecho de los Titulares y su Ejercicio", un capítulo III denominado "Del Derecho al olvido", que regule los aspectos previamente señalados, con el fin primordial de contar con una norma de vanguardia que reconozca, de manera amplia, al derecho de todo individuo a resguardar su intimidad, su honor y su propia imagen.

2. Ley modelo enviada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, envió a esta H. LXII Legislatura del Estado de Zacatecas, el pasado mes de abril del año en curso, la denominada "Ley Modelo Estatal de Protección de Datos Personales". El documento tiene como finalidad servir como guía para que las Legislaturas locales armonicen sus ordenamientos legales en materia de datos personales con lo que dispone la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

En tal sentido, y después de realizar un estudio de derecho comparado, entre las iniciativa de ley en estudio y la Ley modelo, observamos que la estructura es homogénea, pero en algunos puntos en particular, la ley modelo presenta algunas aportaciones que, sin duda, dotarán a la norma reguladora del derecho a la protección de los datos personales en la Entidad, de una estructura lógico-jurídica, idónea para su correcta implementación.

Como consecuencia de lo anterior se proponen las siguientes modificaciones a las iniciativas formuladas por nuestros compañeros legisladores:

A) En el Título Sexto, relativo a las "Acciones Preventivas en Materia de Protección de Datos Personales", se propone se agregue un capítulo II, denominado "Del Oficial de Protección de Datos Personales".

B) En el Título Noveno, denominado "De los Procedimientos de Impugnación en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados", se sugiere se agregue el capítulo II denominado "De los Criterios de Interpretación".

C) En la Ley modelo se amplían las causales de sanción por incumplimiento de las obligaciones en materia de protección de datos, por lo que consideramos importante que en la Ley local se agreguen las siguientes causales:

- Declarar dolosamente la inexistencia de datos personales cuando estos existan total o parcialmente en los archivos del responsable.

- Tratar los datos personales de menara que afecte o impida el ejercicio de los derechos fundamentales previstos en el artículo 29 de la Constitución Política del Estado Libre y Soberano de Zacatecas.

- Realizar actos para intimidar o inhibir a los titulares en el ejercicio de derechos ARCO.

Como corolario a lo anterior, resulta evidente que la iniciativa de Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Zacatecas, se constituye como un ordenamiento vanguardista y armonizado, en contenido y forma, con la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

3. Comunicación Constante con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. De la misma forma, resulta pertinente expresar que esta Comisión de dictamen, por conducto de su Presidente, ha estado en contacto permanente con las autoridades del Instituto Nacional de Transparencia y Acceso a la Información, con el fin de plantear dudas y enriquecer el contenido de la Ley.

Conforme a ello, la citada instancia hizo llegar a esta Comisión algunos comentarios respecto de las iniciativas en estudio, los cuales se han incorporado en el articulado de la Ley, con el fin de lograr, se insiste, su cabal armonización con la Ley General.

En atención a lo anterior, y conforme a las modificaciones que se plantearon previamente, la estructura lógico–jurídica de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Zacatecas, queda integrada de la siguiente manera:

TÍTULO PRIMERO
DISPOSICIONES GENERALES

Capítulo Único
Del Objeto de la Ley

Capítulo Único
Del Procedimiento de Verificación

TÍTULO DÉCIMO PRIMERO
MEDIDAS DE APREMIO Y RESPONSABILIDADES

Capítulo I
De las Medidas de Apremio

Capítulo II
De las Sanciones

T R A N S I T O R I O S

La Ley queda integrada, en su totalidad, por 11 títulos, 134 artículos y cinco artículos transitorios.

Por lo expuesto y fundado, los diputados integrantes de la Comisión de Transparencia y Acceso a la Información Pública de la Honorable Sexagésima Segunda Legislatura del Estado, nos permitimos someter a la consideración del Pleno, el presente Dictamen con proyecto de decreto por el que se expide la

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS DEL ESTADO DE ZACATECAS

TÍTULO PRIMERO
DISPOSICIONES GENERALES

Capítulo Único
Del Objeto de la Ley

Artículo 1. La presente Ley es de orden público y regula la materia de protección de datos personales en posesión de sujetos obligados en el Estado de Zacatecas, de conformidad con lo establecido en los artículos 6° y 16°, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Artículo 2. Son objetivos de la presente Ley:

I. Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso,

rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;

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

III. Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, ayuntamientos, partidos políticos, fideicomisos y fondos públicos del Estado de Zacatecas, con la finalidad de regular su debido tratamiento;

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

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

VI. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley;

VII. Establecer un catálogo de sanciones para aquellas conductas que contravengan las disposiciones previstas en la presente Ley, y

VIII. Promover, fomentar y difundir una cultura de protección de datos personales.

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

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

II. **Aviso de privacidad.** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

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

IV. **Bloqueo.** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de

prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste., se procederá a su cancelación en la base de datos que corresponda;

V. **Comité de Transparencia.** Instancia a la que hace referencia el artículo 27 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas;

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

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

VIII. **Datos personales.** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. Con base en lo anterior, los datos personales los podemos clasificar como:

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

b) **Datos personales biométricos:** Son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población; huellas dactilares, geometría de la mano, análisis del iris, análisis de retina, venas del dorso de la mano, rasgos faciales, patrón de voz, firma manuscrita, dinámica de tecleo, cadencia del paso al caminar, análisis gestual y análisis del ADN;

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

X. **Derecho al olvido.** El derecho que tiene el titular de un dato personal, sus representantes o familiares, para que se borre, bloquee o suprima información de carácter individual cuyo flujo pudiera afectar el libre desarrollo de sus derechos fundamentales, como el derecho a la intimidad, al honor y a la propia imagen**,** y que

se refiera a información obsoleta y sin ninguna utilidad para los fines para los que fue recabada, o por carecer de sentido que se tenga acceso a ella después de un tiempo razonable;

XI. **Días.** Días hábiles;

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

XIII. **Documento de seguridad.** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos persones que posee;
XIV. **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del responsable;

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

XVI. **Ficha signalética.** Documento que contiene datos de identificación de un individuo que se encuentra sujeto a un proceso penal;

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

XVIII. **Instituto Nacional.** Al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XIX. **Instituto.** Instituto Zacatecano de Transparencia, Acceso a la Información y Protección de Datos Personales;

XX. **Ley General.** Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados;

XXI. **Ley.** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Zacatecas;

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

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

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

XXV. **Responsable.** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, ayuntamientos, partidos políticos, fideicomisos y fondos públicos del Estado de Zacatecas, quienes deciden y determinan los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales;

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

XXVII. **Sistema Nacional.** Al Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XXVIII. **Titular.** La persona física a quien corresponden los datos personales;

XXIX. **Transferencia.** Toda comunicación de datos personales dentro o fuera del territorio mexicano, efectuada a persona distinta del titular, del responsable o del encargado;

XXX. **Tratamiento.** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados publicados a los datos personales, relacionadas con la obtención, uso, registros, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento,

posesión, acceso, manejo, aprovechamiento, divulgación, transferencias o disposición de datos personales, y

XXXI. **Unidad de Transparencia.** Instancia a la que se hace referencia en el artículo 29 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas.

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

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

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

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

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

IV. Los medios de comunicación social, y

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

Para que los supuestos enumerados en el presente artículo sean considerados fuentes de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa o sin más exigencia que, en su caso, el pago de una contra prestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.

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

El derecho a la protección de los datos personales será limitado, solamente, por disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Artículo 7. Por regla general no podrán tratarse datos personales, salvo que se cuente con el consentimiento expreso de su titular o, en su defecto, se trate de los casos establecidos en el artículo 16 de esta Ley.

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

Artículo 8. La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales de los que el Estado mexicano sea parte, la Constitución Política del Estado Libre y Soberano de Zacatecas, la Ley General, así como las resoluciones, sentencias, determinaciones, decisiones, criterios y opiniones vinculantes, entre otras, que emitan los órganos nacionales e internacionales especializados.

Artículo 9. En lo no previsto por esta Ley se estará a lo establecido en la Constitución Política de los Estados Unidos Mexicanos en materia de protección de datos personales en posesión de sujetos obligados y, en su caso, en materia de transparencia y derecho de acceso a la información, a lo establecido en la Ley General y, en su caso, a la Ley General de Transparencia y Acceso a la Información Pública; así como a lo establecido en la Constitución Política del Estado Libre y Soberano del Estado de Zacatecas en las materias referidas; la Ley de Transparencia y Acceso a la Información Pública del Estado y la Ley de Procedimiento Administrativo del Estado y Municipios de Zacatecas.

TÍTULO SEGUNDO
PRINCIPIOS, DEBERES Y NIVELES DE SEGURIDAD

Capítulo I
De los Principios

Artículo 10. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Artículo 11. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que le confiera la Ley General, la presente Ley y demás normatividad aplicable.

Artículo 12. Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

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

Artículo 13. El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Artículo 14. Cuando no se actualice alguna de las causales de excepción previstas en el artículo 16 de esta Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

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

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

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

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

Artículo 15. El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.
El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

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

Tratándose de datos personales, sensibles o biométricos, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 16 de esta Ley.

Artículo 16. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

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

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

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

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

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

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

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

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

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

Artículo 17. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

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

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

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

Artículo 18. El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo 17 de esta Ley.

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

Artículo 19. El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Artículo 20. El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

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

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

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

Artículo 21. El aviso de privacidad a que se refiere el artículo 3, fracción II de esta Ley, se pondrá a disposición del titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información:

I. La denominación del responsable;

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

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

IV. Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales;

V. Las finalidades de estas transferencias;

VI. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular;

VII. El sitio donde se podrá consultar el aviso de privacidad integral, y

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

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

Artículo 22. El aviso de privacidad integral, deberá contener, al menos, la siguiente información:

I. El domicilio del responsable;

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

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

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

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

VI. El domicilio de la Unidad de Transparencia, y

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

Artículo 23. El responsable deberá implementar los mecanismos previstos en el artículo 24 de esta Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular del Instituto, debiendo observar la legislación aplicable, para lo cual podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

Artículo 24. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

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

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

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

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

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

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

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra

tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y

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

Capítulo II
De los Deberes

Artículo 25. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Artículo 26. Las medidas de seguridad adoptadas por el responsable deberán considerar:

I. El riesgo inherente a los datos personales tratados;

II. La sensibilidad de los datos personales tratados;

III. El desarrollo tecnológico;

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

V. Las transferencias de datos personales que se realicen;

VI. El número de titulares;

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

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

Artículo 27. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

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

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

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

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

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

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

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

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

Artículo 28. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

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

Artículo 29. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

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

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

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

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

VII. El programa general de capacitación.

Artículo 30. El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

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

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

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

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

Artículo 31. En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Artículo 32. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

I. La pérdida o destrucción no autorizada;

II. El robo, extravío o copia no autorizada;

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

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

Artículo 33. El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo y las acciones correctivas implementadas de forma inmediata y definitiva.

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

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

I. La naturaleza del incidente;

II. Los datos personales comprometidos;

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

IV. Las acciones correctivas realizadas de forma inmediata, y

V. Los medios donde puede obtener más información al respecto.

Artículo 36. El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

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

Capítulo III
De los Niveles de Seguridad

Artículo 37. El Sujeto Obligado responsable de la tutela y tratamiento del sistema de datos personales, adoptará las medidas de seguridad, conforme a lo siguiente:

A. 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 o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados.

B. Niveles de seguridad:

I. **Básico.** Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos:

a) Documento de seguridad;

b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;

c) Registro de incidencias;

d) Identificación y autentificación;

e) Control de acceso;

f) Gestión de soportes; y

g) Copias de respaldo y recuperación.

II. **Medio.** Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos:

a) Responsable de seguridad;

b) Auditoría;

c) Control de acceso físico, y

d) Pruebas con datos reales.

III. **Alto.** Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes al nombre, domicilio particular, CURP RFC, ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de datos a los que corresponde adoptar el nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes, y

b) Registro de acceso;

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

Artículo 38. Las medidas de seguridad a las que se refiere el artículo anterior constituyen mínimos exigibles, por lo que los responsables adoptarán las medidas adicionales que estimen necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales.

Por la naturaleza de la información, las medidas de seguridad que se adopten se comunicarán al Instituto para su registro.

TÍTULO TERCERO
DERECHOS DE LOS TITULARES Y SU EJERCICIO

Capítulo I
De los Derechos de Acceso, Rectificación, Cancelación y Oposición

Artículo 39. En todo momento, el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

Artículo 40. El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

Artículo 41. El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

Artículo 42. El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Artículo 43. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

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

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

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

Artículo 44. La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a los responsables, se sujetará al procedimiento establecido en el presente Título y demás disposiciones que resulten aplicables en la materia.

Artículo 45. Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante.

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

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

Artículo 46. El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable.

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

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

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

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

Artículo 47. El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá

exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

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

Artículo 48. En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:

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

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

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

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

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

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

Artículo 49. Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el artículo anterior, y el responsable no cuente con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco

días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.

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

La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto, para resolver la solicitud de ejercicio de los derechos ARCO.

Artículo 50. Cuando se trate de una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable.

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

Artículo 51. Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto.

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

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

Artículo 52. El Instituto podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.

Artículo 53. Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud y, en caso de poderlo determinar, orientarlo hacia el responsable competente.

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

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

Artículo 54. Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, el responsable deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce tales derechos a través del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado para la atención de solicitudes para el ejercicio de los derechos ARCO conforme a las disposiciones establecidas en este Capítulo.

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

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

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

III. Cuando exista un impedimento legal;

IV. Cuando se lesionen los derechos de un tercero;

V. Cuando se obstaculicen actuaciones judiciales o administrativas;

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

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

VIII. Cuando el responsable no sea competente;

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

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

En los casos anteriores, el responsable deberá informar al titular el motivo de su determinación, en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 47 de la presente Ley y demás disposiciones aplicables, y por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.

Artículo 56. Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 97 de la presente Ley.

Capítulo III
Del Derecho al Olvido

Artículo 57. Sin perjuicio de lo establecido en el capítulo anterior, las personas fallecidas y sujetas a un proceso penal del fuero común, gozarán de las garantías consagradas en el presente capítulo.

Artículo 58. Los responsables que en el ámbito de sus respectivas competencias, manejen, administren y resguarden información personal de personas fallecidas, como datos clínicos e identidad del difunto, deberán guardar estricta cautela de la información, y evitar el mal uso de los datos relativos a su imagen y honor, en términos de la Ley General, la presente Ley y demás ordenamientos aplicables.

Los derechos previstos en el capítulo anterior, podrán ser ejercidos por el representante designado en el testamento del fallecido, a falta de este, por el familiar consanguíneo que acredite su personalidad hasta el cuarto grado de parentesco, o bien, que exista un mandato judicial para dicho efecto.

Artículo 59. Los responsables con funciones jurisdiccionales en el Estado, que resuelvan la inocencia de algún individuo, o bien, se le libere por falta de elementos para procesarlo, además de cancelar su ficha signalética, deberán resguardar cualquier dato que se tenga en sus libros de registro, con el fin de no afectar la vida social y laboral de los individuos.

De la misma forma, en el caso de la información de carácter personal de individuos que hayan sido procesados y condenados por delitos del fuero común, las autoridades jurisdiccionales deberán realizar un manejo adecuado de la información para que esta no se divulgue a terceros ajenos, en términos de lo establecido por el artículo 10 de la presente Ley, con el fin de garantizar que se respeten los derechos fundamentales de la persona que cumplió su sentencia y, en consecuencia, pueda tener un adecuado proceso de reinserción social.

Se exceptuarán de la prohibición de comunicación, los casos en que esa información les sea solicitada por autoridad competente, la que, en todo caso, deberá guardar respecto de ella la debida reserva o secreto en términos de lo previsto por el Titulo Sexto, Capítulo tercero de esta Ley.

Capítulo IV
De la Portabilidad de los Datos

Artículo 60. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

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

Los responsables observarán y atenderán los lineamientos emitidos por el Sistema Nacional, para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

TÍTULO CUARTO
RELACIÓN DEL RESPONSABLE Y ENCARGADO

Capítulo Único
Responsable y Encargado

Artículo 61. El encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable.

Artículo 62. La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

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

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;

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

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

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

V. Guardar confidencialidad respecto de los datos personales tratados;

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

VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

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

Artículo 63. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.

Artículo 64. El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie la autorización expresa de este último. El subcontratado asumirá el carácter de encargado en los términos de la presente Ley y demás disposiciones que resulten aplicables en la materia.

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

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

Artículo 65. Una vez obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que decida, de conformidad con la normatividad que le resulte aplicable, y permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en el presente Capítulo.

Artículo 66. El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

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

Artículo 67. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente:

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

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

c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y

d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

II. Cuente con mecanismos, al menos, para:

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

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

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

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

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

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

TÍTULO QUINTO
COMUNICACIONES DE DATOS PERSONALES

Capítulo Único
De las Transferencias y Remisiones de Datos Personales

Artículo 68. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 16, 69 y 70 de la presente Ley.

Artículo 69. Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

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

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

II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad

extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas o las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

Artículo 70. Cuando la transferencia sea nacional, el receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar la confidencialidad y únicamente utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

Artículo 71. El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obliguen a proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.

Artículo 72. En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular.

Artículo 73. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:

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

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

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

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

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

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

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

VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 16, de la presente Ley.

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

Artículo 74. Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.

TÍTULO SEXTO
ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Capítulo I
De las Mejores Prácticas

Artículo 75. Para el cumplimiento de las obligaciones previstas en la presente Ley, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto:

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

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

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

IV. Facilitar las transferencias de datos personales;

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

VI. Demostrar ante el Instituto, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

Artículo 76. Todo esquema de mejores prácticas que busque la validación o reconocimiento por parte del Instituto deberá:

I. Cumplir con los parámetros que para tal efecto emita el Instituto conforme a los criterios que fije el Instituto Nacional, y

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

El Instituto, deberá emitir las reglas de operación de los registros en los que se inscribirán aquellos esquemas de mejores prácticas validados o reconocidos. El Instituto, podrá inscribir los esquemas de mejores prácticas que hayan reconocido o validado en el registro administrado por el Instituto Nacional, de acuerdo con las reglas que fije este último.

Artículo 77. Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de Impacto en la protección de datos personales, y presentarla ante el Instituto, el cual podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

Artículo 78. Para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

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

II. Se traten datos personales sensibles o biométricos, y

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

Artículo 79. Los responsables que realicen una Evaluación de Impacto en la protección de datos personales, deberán presentarla ante el Instituto, treinta días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, ante el Instituto a efecto de que emitan las recomendaciones no vinculantes correspondientes.

Artículo 80. El Instituto deberá emitir, de ser el caso, recomendaciones no vinculantes sobre la Evaluación de Impacto en la protección de datos personales

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

Artículo 81. Cuando a juicio del Sujeto Obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la Evaluación de Impacto en la protección de datos personales.

Capítulo II
Del Oficial de Protección de Datos Personales

Artículo 82. Los responsables deberán designar a un oficial de protección de datos personales, quien será la persona encargada de tratar los datos personales en términos de la Ley General, la presente Ley y demás disposiciones aplicables, el cual podrá acudir a las sesiones del Comité de Transparencia de cada responsable, a petición del presidente, cuando el tema que se trate lo vincule.

La persona designada como oficial de protección de datos deberá contar con la jerarquía o posición dentro de la organización del responsable que le permita implementar políticas transversales en esta materia.

Artículo 83. El oficial de protección de datos personales será designado atendiendo a su experiencia y cualidades profesionales, en particular, a sus conocimientos en la materia y deberá contar con recursos suficientes para llevar a cabo su cometido.

Artículo 84. El oficial de protección de datos personales tendrá las siguientes atribuciones:

I. Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;

II. Diseñar, ejecutar, supervisar y evaluar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia, en coordinación con el Comité de Transparencia;

III. Asesorar permanentemente a las áreas de cada Sujeto Obligado en materia de protección de datos personales, y

IV. Las que determine la normatividad aplicable.

Capítulo III
De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia

Artículo 85. La obtención y tratamiento de datos personales, en términos de los que dispone esta Ley, por parte de los responsables competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto.

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

Artículo 86. En el tratamiento de datos personales, así como en el uso de las bases de datos para almacenamiento, que realicen los responsables competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los propósitos establecidos en el Título Segundo de la presente Ley.

Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad competente que faculte la ley o del titular del Ministerio Público del Estado podrá autorizar la intervención de cualquier comunicación privada.

Artículo 87. Los responsables de las bases de datos a que se refiere este Capítulo, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

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

Capítulo I
Comité de Transparencia

Artículo 88. Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas y demás normativa aplicable.

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

Artículo 89. Para los efectos de la presente Ley, y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:

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

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

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

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

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

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto;

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

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

Capítulo II
De la Unidad de Transparencia

Artículo 90. Cada responsable contará con una Unidad de Transparencia, que se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia y Acceso

a la Información Pública del Estado de Zacatecas, la presente Ley y demás normatividad aplicable.

Sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, para los efectos de la presente Ley, la Unidad de Transparencia tendrá las siguientes funciones:

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

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

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

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

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

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

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

En caso de ser requerido, los responsables podrán solicitar el apoyo de instituciones, asociaciones, fundaciones y demás organismos especializados, que pudieran auxiliarles en el trámite de las respuestas a solicitudes de información, en lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

Artículo 91. El responsable procurará contar con la infraestructura y los medios tecnológicos necesarios para garantizar que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.

Artículo 92. En la designación del titular de la Unidad de Transparencia, el responsable estará a lo dispuesto en la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas y demás normativa aplicable.

TÍTULO OCTAVO
DE LA AUTORIDAD RESPONSABLE

Capítulo I
Del Instituto Zacatecano de Transparencia, Acceso a la Información y Protección de Datos Personales

Artículo 93. El Instituto es un organismo público autónomo con personalidad jurídica y patrimonio propios, con autonomía en sus funciones e independencia en sus decisiones; tiene como atribuciones, promover la transparencia, garantizar el acceso a la información pública de libre acceso y proteger los datos personales en posesión de los responsables.

En la integración, procedimiento de designación y funcionamiento del Instituto se estará a lo dispuesto por la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas y demás normativa aplicable.

Artículo 94. Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que resulte aplicable, el Instituto tendrá las siguientes atribuciones:

I. Garantizar el ejercicio del derecho a la protección de datos personales en posesión de los responsables;

II. Interpretar la presente Ley en el ámbito administrativo;

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

IV. Conocer, sustanciar y resolver los procedimientos de verificación;

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

VI. Establecer y ejecutar las medidas de apremio previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia;

VII. Elaborar formatos guía para toda la población y los responsables sobre los temas siguientes, entre otros:

VIII. Realizar solicitudes para el ejercicio de los derechos ARCO.

IX. Recurso de revisión;

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

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

XII. Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia en la presente Ley;

XIII. Hacer del conocimiento de las autoridades competentes, la probable responsabilidad derivada del incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones que resulten aplicables;

XIV. Proporcionar al Instituto Nacional los elementos que requiera para resolver los recursos de inconformidad que le sean presentados, en términos de lo previsto por la Ley General, y demás disposiciones que resulten aplicables en la materia;

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

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

XVII. Emitir las autorizaciones previstas en la presente Ley, la Ley General y demás disposiciones aplicables;

XVIII. Solicitar la cooperación del Instituto Nacional en los términos del artículo 89, fracción XXX de la Ley General de Protección de Datos en Posesión de Sujetos Obligados;

XIX. Administrar, en el ámbito de su competencia, la Plataforma Nacional de Transparencia;

XX. Aprobar, a propuesta del Presidente del Consejo Consultivo, los reglamentos, lineamientos, manuales de procedimientos, políticas y demás normas que resulten necesarias para la instrumentación de la presente Ley;

XXI. Según corresponda, interponer acciones de inconstitucionalidad en contra de leyes expedidas por la Legislatura del Estado que vulneren el derecho a la protección de datos personales;

XXII. Emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de Impacto en protección de datos personales que le sean presentadas.

XXIII. Vigilar, en el ámbito de su competencia, el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia; y

XXIV. Las demás que establezcan otras disposiciones legales y reglamentarias aplicables.

Capítulo II
De la Coordinación y Promoción del Derecho a la Protección de Datos Personales

Artículo 95. Los responsables deberán colaborar con el Instituto, para capacitar y actualizar, de forma permanente, a todos sus servidores públicos en materia de protección de datos personales, a través de la impartición de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.

Artículo 96. El Instituto deberá, en coordinación con los responsables:

I. Promover y difundir el derecho de protección de datos personales, haciéndolo accesible a cualquier persona y desarrollando políticas activas de difusión;

II. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de datos personales, los procesos de protección y denuncia;

III. Promover la capacitación y actualización de los responsables en sus obligaciones respecto al tratamiento de datos personales en su posesión;

IV. Promover la impartición del tema de protección de datos personales, a través de clases, talleres, pláticas y foros en educación preescolar, primaria, secundaria y media superior;

V. Promover la cultura de la protección de datos personales para impulsar la inclusión en el sistema educativo estatal y de educación superior, de programas, planes de estudio, asignaturas, libros y materiales que fomenten entre los alumnos la importancia del cuidado, ejercicio y respeto de sus datos personales, así como las obligaciones de las autoridades y de las propias personas al respecto;

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

VII. Fomentar la creación de espacios de participación social y ciudadana que estimulen el intercambio de ideas entre la sociedad y los responsables.

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

Capítulo Único
Del Recurso de Revisión ante el Instituto

Artículo 97. El titular, por sí mismo o a través de su representante, podrá interponer el recurso de revisión ante el Instituto o la Unidad de Transparencia del responsable que haya conocido de la solicitud para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta.

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

Artículo 98. El recurso de revisión procederá en los siguientes supuestos:

I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

II. Se declare la inexistencia de los datos personales;

III. Se declare la incompetencia por el responsable;

IV. Se entreguen datos personales incompletos;

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

VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales;

VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia;

VIII. Se entreguen o pongan a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;

IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;

X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;

XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y

XII. En los demás casos que dispongan las leyes.

Artículo 99. Los únicos requisitos exigibles en el escrito de interposición del recurso de revisión serán los siguientes:

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

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

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

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

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

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

Al recurso de revisión se podrán acompañar las pruebas y demás elementos que considere el titular procedentes someter a juicio del Instituto.

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

Artículo 100. Una vez admitido el recurso de revisión, el Instituto podrá buscar una conciliación entre el titular y el responsable. De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto, deberá verificar el cumplimiento del acuerdo respectivo.

Artículo 101. Admitido el recurso de revisión y sin perjuicio de lo dispuesto por el artículo 68 de la presente Ley, el Instituto promoverá la conciliación entre las partes, de conformidad con el siguiente procedimiento:

I. El Instituto requerirá a las partes que manifiesten, por cualquier medio, su voluntad de conciliar, en un plazo no mayor a siete días, contados a partir de la notificación de dicho acuerdo, mismo que contendrá un resumen del recurso de revisión y de la respuesta del responsable si la hubiere, señalando los elementos comunes y los puntos de controversia.

La conciliación podrá celebrarse presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el Instituto. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.

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

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

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

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

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

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

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

V. De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto, deberá verificar el cumplimiento del acuerdo respectivo, y

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

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

Artículo 102. El Instituto resolverá el recurso de revisión en un plazo que no podrá exceder de cuarenta días, el cual podrá ampliarse hasta por veinte días por una sola vez.

Artículo 103. Durante el procedimiento a que se refiere el presente Capítulo, el Instituto deberá aplicar la suplencia de la queja a favor del titular, siempre y cuando no altere el contenido original del recurso de revisión, ni modifique los hechos o peticiones expuestas en el mismo, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones.

Artículo 104. Si en el escrito de interposición del recurso de revisión el titular no cumple con alguno de los requisitos previstos en el artículo 99 de la presente Ley y el Instituto no cuenta con elementos para subsanarlos, éste deberá requerir al titular, por una sola ocasión, la información que subsane las omisiones en un plazo que no

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

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

Artículo 105. Las resoluciones del Instituto podrán:

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

II. Confirmar la respuesta del responsable;

III. Revocar o modificar la respuesta del responsable, o

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

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

Ante la falta de resolución por parte del Instituto, se entenderá confirmada la respuesta del responsable.

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

Artículo 106. El recurso de revisión podrá ser desechado por improcedente cuando:

I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 97 de la presente Ley;

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

III. El Instituto haya resuelto anteriormente en definitiva sobre la materia del mismo;

IV. No se actualice alguna de las causales del recurso de revisión previstas en el artículo 98 de la presente Ley;

V. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el recurrente, o en su caso, por el tercero interesado, en contra del acto recurrido ante el Instituto;

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

VII. El recurrente no acredite interés jurídico.

El desechamiento no implica la preclusión del derecho del titular para interponer ante el Instituto un nuevo recurso de revisión.

Artículo 107. El recurso de revisión solo podrá ser sobreseído cuando:

I. El recurrente se desista expresamente;

II. El recurrente fallezca;

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

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

V. Quede sin materia el recurso de revisión.

Artículo 108. El Instituto deberá notificar a las partes y publicar las resoluciones, en versión pública, a más tardar, al tercer día siguiente de su aprobación.

Artículo 109. Las resoluciones del Instituto serán vinculantes, definitivas e inatacables para los responsables.

Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el juicio de amparo.

Artículo 110. Tratándose de las resoluciones que emita el Instituto, los particulares podrán optar por acudir ante el Instituto Nacional interponiendo el recurso de inconformidad previsto en la Ley General o ante el Poder Judicial de la Federación mediante el juicio de amparo.

Artículo 111. El recurso de inconformidad y la facultad de atracción que posee el Instituto Nacional, se sustanciarán conforme el procedimiento descrito en la Ley General de Protección de Datos Personales y demás leyes reglamentarias.

Artículo 112. Una vez que hayan causado ejecutoria las resoluciones dictadas en los recursos que se sometan a su competencia, el Instituto podrá emitir los criterios de interpretación que estime pertinentes y que deriven de los resuelto en dichos asuntos.

TÍTULO DÉCIMO
FACULTAD DE VERIFICACIÓN DEL INSTITUTO

Capítulo Único
Del Procedimiento de Verificación

Artículo 113. El Instituto tendrá la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley General, la presente Ley y demás ordenamientos que se deriven de ésta.

En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto estará obligado a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.

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

Artículo 114. La verificación podrá iniciarse:

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

II. Por denuncia del titular, cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable o, en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia.

El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la

misma. Cuando los hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado.

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

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

Artículo 115. Para la presentación de una denuncia no podrán solicitarse mayores requisitos que los que a continuación se describen:

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

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

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

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

V. La firma del denunciante o, en su caso, de su representante. En caso de no saber firmar, bastará la huella digital.

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

Una vez recibida la denuncia, el Instituto deberá acusar recibo de la misma. El acuerdo correspondiente se notificará al denunciante.

Artículo 116. La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación o realizar visitas a las oficinas o instalaciones del responsable o, en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.

Para la verificación en instancias de seguridad pública en el ámbito estatal, se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados; así como de una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información solo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 117.

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

El Instituto podrá ordenar medidas cautelares, si del desahogo de la verificación advierten un daño inminente o irreparable en materia de protección de datos personales, siempre y cuando no impidan el cumplimiento de las funciones ni el aseguramiento de bases de datos de los responsables.

Estas medidas solo podrán tener una finalidad correctiva y será temporal hasta en tanto los responsables lleven a cabo las recomendaciones hechas por el Instituto.

Artículo 117. El procedimiento de verificación concluirá con la resolución que emita el Instituto, en la cual se establecerán las medidas que deberá adoptar el responsable en el plazo que en ella se determine.

Artículo 118. Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General, la presente Ley y demás normativa que resulte aplicable.

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

TÍTULO DÉCIMO PRIMERO
MEDIDAS DE APREMIO Y RESPONSABILIDADES

Capítulo I
De las Medidas de Apremio

Artículo 119. El Instituto podrá imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

I. La amonestación pública, o

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

El incumplimiento de los responsables será difundido en los portales de obligaciones de transparencia del Instituto, considerados en las evaluaciones que realicen éstos.

En caso de que el incumplimiento de las determinaciones del Instituto, implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 129 de la presente Ley, deberán denunciar los hechos ante la autoridad competente.

Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 120. Si a pesar de la ejecución de las medidas de apremio previstas en el artículo anterior no se cumpliere con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora.

De persistir el incumplimiento, se aplicarán, sobre aquéllas, las medidas de apremio establecidas en el artículo anterior.

Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista la autoridad competente en materia de responsabilidades.

Artículo 121. Las medidas de apremio a que se refiere el presente Capítulo, deberán ser aplicadas por el Instituto o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.

Artículo 122. Las multas que fije el Instituto, se harán efectivas por la Secretaría de Finanzas del Estado, a través de los procedimientos que las leyes establezcan.

Artículo 123. Para calificar las medidas de apremio establecidas en el presente Capítulo, el Instituto deberá considerar:

I. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto y la afectación al ejercicio de sus atribuciones;

II. La condición económica del infractor, y

III. La reincidencia.

El Instituto establecerá, mediante lineamientos de carácter general, las atribuciones de las áreas encargadas de calificar la gravedad de la falta de observancia a sus determinaciones y de la notificación y ejecución de las medidas de apremio que apliquen e implementen, conforme a los elementos desarrollados en este Capítulo.

Artículo 124. En caso de reincidencia, el Instituto podrá imponer una multa equivalente hasta el doble de la que se hubiera determinado por el Instituto.

Se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.

Artículo 125. Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.

Artículo 126. La amonestación pública será impuesta por el Instituto y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.

Artículo 127. El Instituto podrá requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base en los elementos que se tengan a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de Internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto para requerir aquella documentación que se considere indispensable para ese efecto a las autoridades competentes.

Artículo 128. En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante la autoridad jurisdiccional competente.

Capítulo II
De las Sanciones

Artículo 129. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, y de manera indebida, datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 21 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;

VII. Incumplir el deber de confidencialidad establecido en el artículo 36 de la presente Ley;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 25, 26 y 27 de la presente Ley;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad, según los artículos 25, 26 y 27 de la presente Ley;

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

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;

XIII. No acatar las resoluciones emitidas por el Instituto;

XIV. Declarar dolosamente la inexistencia de datos personales cuando estos existan total o parcialmente en los archivos del responsable;

XV. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales previstos en el artículo 29 de la Constitución Política del Estado Libre y Soberano de Zacatecas;

XVI. Realizar actos para intimidar o inhibir a los titulares en el ejercicio de derechos ARCO, y

XVII. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 28, fracción VII de la Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas, o bien, entregar el mismo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, XIV, XV, XVI y XVII, así como la reincidencia en las conductas previstas en el resto de

las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 130. Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que imponga o ejecute la sanción.

Artículo 131. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 129 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto podrá denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

Artículo 132. Ante incumplimientos por parte de los partidos políticos, el Instituto dará vista, al Instituto Electoral del Estado de Zacatecas, para que resuelvan lo conducente, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.

En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto deberá dar vista al órgano interno de control del Sujeto Obligado relacionado con éstos, cuando sean servidores públicos, con el fin de que instrumenten los procedimientos administrativos a que haya lugar.

Artículo 133. En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.

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

A efecto de sustanciar el procedimiento citado en este artículo, el Instituto deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad.

Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La denuncia y el expediente deberán remitirse a la contraloría, órgano interno de control o equivalente dentro de los quince días siguientes a partir de que el Instituto tenga conocimiento de los hechos.

Artículo 134. En caso de que el incumplimiento de las determinaciones del Instituto impliquen la presunta comisión de un delito, el Instituto deberá denunciar los hechos ante la autoridad competente.

T R A N S I T O R I O S

PRIMERO. La presente Ley entrará en vigor al día siguiente de su publicación en el Periódico Oficial, Órgano de Gobierno del Estado de Zacatecas.

SEGUNDO. Se derogan todas aquellas disposiciones en materia de protección de datos personales, que contravengan lo dispuesto en la presente Ley.

TERCERO. Los responsables expedirán sus avisos de privacidad en los términos previstos en la presente Ley y demás disposiciones aplicables, a más tardar sesenta días posteriores a la entrada en vigor de esta Ley.

CUARTO. Los procedimientos iniciados durante la vigencia de la ley que resulte aplicable en materia de protección de datos personales del estado de Zacatecas se sustanciarán hasta su conclusión, conforme al ordenamiento señalado.

QUINTO. El Instituto deberá expedir los lineamientos, parámetros, criterios y demás disposiciones de las diversas materias a que se refiere la presente Ley, dentro de los 180 días siguientes a la entrada en vigor del presente Decreto.

Así lo dictaminaron y firman los Diputados integrantes de la Comisión de Transparencia y Acceso a la Información Pública de la Honorable Sexagésima Segunda Legislatura del Estado.

LXII LEGISLATURA
ESTADO DE ZACATECAS
2016 • 2018

Zacatecas, Zac., 20 de junio de 2017.

COMISIÓN DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

H. LXII LEGISLATURA DEL ESTADO DE ZACATECAS

DIP. JORGE TORRES MERCADO
Presidente

DIP. GUADALUPE CELIA FLORES ESCOBEDO
Secretaria

DIP. MA. GUADALUPE GONZÁLEZ MARTÍNEZ
Secretaria