

**COMISIÓN DE INFORMACIÓN PÚBLICA
Y PROTECCIÓN DE DATOS PERSONALES**

HONORABLE ASAMBLEA:

Los que suscriben, Diputados integrantes de la Comisión de Información Pública y Protección de Datos Personales del Congreso del Estado de Tlaxcala, con fundamento en lo dispuesto por los artículos 45, 46 fracción I, 54 fracción I de la Constitución Política del Estado Libre y Soberano de Tlaxcala; 78, 80, 81 y 82 fracción XXVI de la Ley Orgánica del Poder Legislativo del Estado de Tlaxcala; 35, 36, 37 fracción XXVI, 38 fracción III, 62 Bis fracción III, 115, 124 y 125 del Reglamento Interior del Congreso del Estado, nos permitimos presentar ante el Pleno de esta Soberanía la siguiente Iniciativa con carácter de Dictamen con Proyecto de Ley de Protección de Datos Personales para el Estado de Tlaxcala, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

1. En fecha veintisiete de abril de dos mil once, la Comisión signante, en coordinación con el Consejo General de la Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala, con el objeto de contribuir a generar entre la sociedad una cultura de reconocimiento y respeto de los derechos de acceso a la

información y el de protección de datos personales, llevamos a cabo el Foro intitulado “Protección de Datos Personales...una responsabilidad compartida”. Cabe destacar que dentro de la ponencia magistral disertada por el subdirector de la Dirección de Datos Personales del Instituto de Acceso a la Información Pública del Distrito Federal, Ignacio Núñez Ruiz, se hizo patente la necesidad de realizar una profunda reforma en materia de protección de datos personales y acceso a la información, sugiriendo dicho ponente la creación de dos leyes que avalen, por separado estos derechos.

2. En coincidencia con la propuesta formulada por el maestro Ignacio Núñez Ruiz, esta Comisión comenzó los trabajos legislativos tendientes a separar estos dos derechos, por lo que en fecha catorce de junio de dos mil once, en el Salón Blanco de este recinto legislativo, contando con la presencia de los Comisionados del Consejo General de la Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala, la Presidencia de la Comisión de mérito, celebró la instalación de la mesa de trabajo en la que se presentó la propuesta de iniciativa de Ley de Protección de Datos Personales para el Estado de Tlaxcala, elaborada por el Diputado Francisco Javier Romero Ahuactzi, Presidente de la Comisión de Información Pública y Protección de Datos Personales del Congreso del Estado. En esta reunión, se hizo patente el interés de los Comisionados así como de la Presidencia de la Comisión que suscribe, por proteger el derecho que tienen todos los individuos a mantener fuera del conocimiento público aspectos de la vida personal, tales como son la convivencia familiar, la conducta sexual y afectiva, las creencias religiosas, el patrimonio personal, entre otros.

3. Derivado de esta primera reunión de trabajo, en fecha veintiuno de junio del año dos mil once, en las instalaciones de la Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala, contando con la presencia de los Comisionados Maestro Miguel Ángel Carro Aguirre, Maestra Mayra Romero Gaytán y Maestro Claudio Cirio Romero, se llevó a cabo la segunda mesa de trabajo cuyo objetivo fue el de realizar un estudio comparado de la propuesta primigenia y de la propia propuesta formulada por los Comisionados, con el objeto de encontrar similitudes y coincidencias y así elaborar un proyecto en el que se recogieran las inquietudes de ambas entidades públicas.
4. De esta forma, al contar con un primer borrador de Ley de Protección de Datos Personales para el Estado de Tlaxcala, aprobado tanto por los Comisionados de la Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala así como por la Presidencia de la Comisión de Información Pública y Protección de Datos Personales del Congreso del Estado, se convocó a una nueva mesa de trabajo a celebrarse en las instalaciones que albergan el Salón Blanco del Recinto Oficial del Poder Legislativo del Estado de Tlaxcala. Como resultado de esta mesa de trabajo, y una vez que se sometió a consideración de los comisionados y de los propios diputados promoventes el contenido de la presente iniciativa con carácter de dictamen con proyecto de Ley, se obtuvieron las observaciones y comentarios que sirvieron para enriquecer la Iniciativa de mérito.
5. A partir de las mesas de trabajo a que se ha hecho referencia en los puntos anteriores, esta Comisión elaboró la iniciativa con carácter de dictamen con proyecto de Ley de Protección de Datos Personales para el

Estado de Tlaxcala, al que se le dio primera lectura en la sesión ordinaria del Pleno de esta Soberanía, celebrada en fecha cuatro de octubre de dos mil once.

6. Con fecha cinco de octubre de dos mil once, por conducto de la Presidencia de esta Comisión Dictaminadora, fue remitido a los diputados integrantes de esta LX Legislatura, copia de la iniciativa con carácter de dictamen con proyecto de Ley de Protección de Datos Personales para el Estado de Tlaxcala, para efectos de que conocieran a fondo el contenido y alcances del ordenamiento legal de marras y al mismo tiempo, y de considerarlo pertinente, remitieran a la Presidencia de esta Comisión, sus observaciones y propuestas. Fue así como se recibieron las propuestas de los diputados Tulio Larios Aguilar, Héctor Martínez García y Justo Lozano Tovar, quienes formularon diversas observaciones al contenido del Dictamen de Ley de Protección de Datos Personales para el Estado de Tlaxcala. De igual forma, en el mes de enero de esta anualidad, fueron recibidas las observaciones formuladas por los diputados Mario Hernández Ramírez y Silvestre Velásquez Guevara, así como del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.
7. Teniendo como sustento las propuestas recibidas por los diputados antes referidos, esta Comisión Dictaminadora sometió al Pleno de esta Soberanía un Proyecto de Acuerdo por el que se retira del proceso legislativo la iniciativa con carácter de dictamen con proyecto de Ley de Protección de Datos Personales para el Estado de Tlaxcala, dada a conocer en fecha cuatro de octubre de dos mil once, siendo aprobado dicho retiro. Por lo que en mérito de lo anterior, esta Comisión

Dictaminadora no presenta impedimento legal alguno para presentar ante el Pleno del Congreso del Estado, un nuevo dictamen de Ley de Protección de Datos Personales para el Estado de Tlaxcala, en el que se han incluido las propuestas formuladas por los legisladores antes mencionados y por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, mismas que han servido para enriquecer el contenido normativo de este nuevo ordenamiento legal, que de ser aprobado, contribuirá en la consolidación de un estado democrático y colocará a Tlaxcala dentro del grupo selecto de entidades que integran el territorio nacional, que cuentan con un ordenamiento legal que permite garantizar a los individuos el respeto y la protección irrestricta de sus datos personales.

8. Es preciso mencionar que la elaboración de la presente iniciativa con carácter de Dictamen de Ley, tiene sustento en los antecedentes mundiales y nacionales que han dado pauta al reconocimiento del derecho de protección de datos personales. Así las cosas, En 1888, en el siglo XIX, Thomas Mc Intyre Cooley habló ya de *“the right to be let alone*, el derecho a ser dejado en paz y poder disfrutar libremente de la privacidad o el derecho a la soledad”.

En 1890, Samuel Warren y Luis Brandeis, publican en Harvard Law Review, su famoso artículo The Right to Privacy. En aquel entonces los autores hablaban de un nuevo derecho: el derecho a poder vivir solo, a que le dejen a uno solo en su vida.

Este es uno de los contenidos esenciales del derecho fundamental a la protección de datos en sus orígenes: el construir una esfera de intimidad, que les permita a las personas ser dueños de su propia privacidad.

Una primera aproximación a la protección de la esfera íntima de las personas, lo fue la Declaración Universal de los Derechos Humanos, del año 1948. En el artículo 12 de esta Declaración se establece que “nadie podrá ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia; ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

De esta forma, dicho enunciado normativo ha servido de sustento para que en las diversas legislaciones nacionales se adopte el reconocimiento del derecho a la intimidad o privacidad de las personas.

En 1967 se constituyó, en el seno del Consejo de Europa, una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a no sufrir injerencias en la vida privada, derecho que se había ya recogido en la Declaración Universal de Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos del año 1966.

De tal comisión consultiva surge la Resolución 506 de la Asamblea del Consejo de Europa, sobre los derechos humanos y los nuevos logros científicos y técnicos, que respondía a una inquietud existente en todo el Continente. Suele decirse, no sin razón, que en tal resolución se

encuentra el verdadero origen del movimiento legislativo que desde entonces recorrerá Europa y el mundo entero, en materia de protección de datos.

También es necesario citar la Ley Land de Jesse, pionera en la materia, la Ley Federal Alemana del año 1977 y la Ley Francesa en Informática Ficheros y Libertades de 1978.

Por su parte, la OCDE también publica dos importantes recomendaciones: La recomendación sobre circulación internacional de datos personales para la protección de la intimidad y la relativa a la seguridad de los sistemas de información.

Ya durante los años noventa se produce, además, un importante movimiento regulatorio, no sólo en Europa sino en muchos países; en España se aprueba la primera Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, sólo referida al tratamiento automatizado de datos personales en el año noventa y dos. En esa misma década, en mil novecientos noventa y tres, la Constitución de Perú reconoce el derecho de acceso a la información y el derecho a la intimidad; por su parte, la Constitución de Brasil y la ley brasileña del año noventa y siete reconocen el Data, mientras que en mil novecientos noventa y nueve en la Constitución venezolana se reconocen los derechos de acceso, rectificación y cancelación a los datos personales y en el mismo año se aprueba la ley chilena de protección de la vida privada. Por su parte, en el noventa y ocho la Constitución de Ecuador reconoce los derechos de acceso, rectificación y cancelación.

9. Por cuanto hace a nuestro país, desde 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, mas tarde lo fue, el secreto a las comunicaciones privadas. Todos estos derechos se encuentran vinculados con la intimidad de la persona, pues protegen ciertas áreas o espacios relativos a todo ser humano. Sin embargo, hoy en día, el reconocimiento de un catalogo abierto de derechos y con el creciente avance tecnológico, ha sido necesario dar respuesta a las nuevas pretensiones individuales, consecuencia de los cambios sociales que la informática ha ido introduciendo.

En materia de protección de datos personales, México y Tlaxcala, en lo particular, han realizado los primeros esfuerzos. En el ámbito federal, la primera aproximación a la protección de datos personales se dio con la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública, en el año 2002, al establecer en su artículo 3 que:

“Para los efectos de esta Ley se entenderá por [...]

*II. **Datos Personales:** La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología opiniones políticas, creencias o convicciones religiosas filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.*

De la interpretación literal del artículo 3 de dicha Ley aprobada en el año 2002, se colige que el legislador hizo referencia al uso y destino de los datos personales, por lo que en el caso del derecho a la intimidad, la alusión que realiza la Ley en lo referente a los datos personales, es de forma y no de fondo, por lo que podría considerarse que tanto el derecho a la intimidad como la protección de datos son derechos diversos. Ciertamente el contenido de ambas parte de la idea de la dignidad. Esto es, en lo referente a la protección de datos, se trata de brindar protección a toda aquella información que para la persona es considerada como íntima.

Debe quedar claro que la protección de datos personales es un derecho fundamental independiente del derecho a la intimidad, tal como se ha puesto de manifiesto en el territorio europeo. Siendo este el modelo que se ha venido implementando por la gran mayoría de los países preocupados en el reconocimiento de la protección de datos personales.

Posterior a la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública, del año 2002, el legislador federal promovió las reformas a la Constitución Política de los Estados Unidos Mexicanos, con el objeto de reconocer los derechos de acceso a la información pública y de protección de datos personales. De esta forma, mediante decreto publicado en el Diario Oficial de la Federación, de fecha veinte de julio de dos mil siete, se adicionó un segundo párrafo con siete fracciones al artículo 6 de nuestra Carta Magna cuyo objeto fue el de **establecer los principios y bases sobre los que la Federación, los Estados y el**

Distrito Federal, regirán el ejercicio del derecho de acceso a la información y la protección de datos personales.

Como resultado de dicha reforma constitucional, en las fracciones II y III del segundo párrafo del artículo 6 se estableció la obligación de proteger la información que se refiera a la vida privada y a los datos personales, mediante la aplicación de las leyes de la materia que a nivel federal como de los estados fueran elaboradas para tal fin. Al mismo tiempo, se otorgaba reconocimiento de los derechos ARCO, o derechos de acceso, rectificación, cancelación u oposición de datos personales.

Por otra parte, mediante la adición de un segundo párrafo al artículo 16 Constitucional, el legislador federal elevó al rango de garantía constitucional el derecho a la protección de los datos personales, el acceso, rectificación y cancelación así como a manifestar su oposición de los mismos. De esta forma el nuevo segundo párrafo del artículo en mención, estableció:

“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 a proteger los derechos de terceros”.

Como consecuencia de dichas reformas constitucionales, en el ámbito federal, mediante Decreto publicado en el Diario Oficial de la Federación el cinco de julio de dos mil diez, entró en vigor el cinco de julio del año dos mil once la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, cuyo objeto es el de proteger 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.

- 10.** Por cuanto se refiere al ámbito estatal, una primera aproximación al reconocimiento y a la protección de datos personales se encuentra en la Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala, aprobada por la LVIII Legislatura del Congreso del Estado, mediante Decreto número 108, de fecha catorce de diciembre de dos mil seis. En este ordenamiento jurídico, si bien el legislador al entrar en una dinámica globalizadora, reconoció la importancia que a nivel mundial revestía el reconocimiento de dos derechos fundamentales como lo son el de acceso a la información y el de protección de datos personales, consideró que tratándose de derechos de nueva creación debían estar regulados por una sola norma.

De esta forma, en el cuerpo de dicha Ley, de manera general se reconoce el derecho de los individuos a la protección de sus datos personales pero no existe disposición expresa sobre los procedimientos para el ejercicio de los derechos ARCO, sobre los principios que han de regir la tutela y el ejercicio de estos derechos, así como las funciones que

la autoridad encargada de velar por su cumplimiento debe adoptar frente a las entidades públicas.

De manera posterior, mediante reforma constitucional, en el inciso c) de la fracción V del artículo 19 de la Ley Suprema Estatal, se elevó a rango constitucional el reconocimiento del derecho que todas las personas tienen para acceder a sus datos personales o a la rectificación de éstos.

11. Como corolario de los antecedentes narrados, se puede señalar que no obstante que en diversos momentos y lugares del mundo se ha puesto especial cuidado en el reconocimiento y protección de la intimidad o privacidad de las personas, en los trabajos legislativos que se han realizado para alcanzar el pleno reconocimiento del derecho de protección de datos personales aún hay mucho por hacer. Un primer ejercicio que resultó de vital importancia para la redacción de esta iniciativa fue el definir lo que se debe entender por “protección de datos personales”.

En este aspecto definitorio, se considera conveniente evocar la definición acuñada por Hondius, quien señala que la protección de datos es “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”.

A partir de este concepto se puede inferir que el tema de la protección de la privacidad de los datos personales, es un tema que se caracteriza por su interdisciplinariedad, por lo que, en palabras de la Doctora María Alejandra Sepúlveda Toro, *“la naturaleza jurídica de este derecho es sui*

généris, pues no hay un derecho absoluto de dominio sobre la información por parte del titular, ya que éste puede adquirir un carácter de supraindividual, cuando el conocimiento de esa información sea necesaria para la protección de su titular o responda a fines superiores establecidos por el bien común”.

Partiendo de lo referido por la doctrina, es evidente que, al estarnos refiriendo a datos personales, no sólo nos referimos a los datos íntimos, no sólo los datos que afecten a la privacidad, sino cualquier tipo de dato personal, por lo que, el contenido del derecho implica que cada ciudadano es dueño de sus datos personales, sean éstos o no íntimos, por tanto hablamos de datos personales, y hablamos de datos personales que estén sometidos a tratamiento informatizado o no informatizado; para decirlo más simplemente: que estén incorporados a un archivo, fichero, registro o sistema de datos, sea este informatizado o no.

12. Como consecuencia de la conceptualización de este nuevo derecho, también es de suma importancia el poder diferenciar entre dos aspectos: el derecho a la intimidad y el derecho a la protección de datos personales. Respecto del primero de ellos, debe decirse que, es el derecho que se refiere a una esfera privada de la persona, mientras que el derecho a la protección de los datos personales en parte presume el tratamiento de la información sobre las personas, hace que esa información no sea secreta, sino todo lo contrario, que sea objeto de un tratamiento, inclusive de un tratamiento masivo, pero exige una conducta activa por parte de los que realizan ese tratamiento y esa conducta activa

consiste básicamente en que sea una conducta o un tratamiento con garantías, una conducta garantista.

- 13.** A partir de la conceptualización del derecho de protección de datos personales y su diferenciación con otros derechos como lo es el derecho a la intimidad y, partiendo de aquel reconocimiento que el legislador federal ha otorgado a dicho derecho al grado tal de elevarlo a rango constitucional como una garantía más del individuo, ahora bien, es ineludible reconocer que la protección de los datos personales constituye uno de los elementos fundamentales de cualquier ordenamiento que se proponga proteger los derechos y libertades de los ciudadanos, por lo que una consolidación normativa y doctrinal del llamado derecho a la autodeterminación informativa deberá propiciar la aparición de instituciones que permitan al ciudadano controlar los usos que las entidades públicas hacen de sus datos.

Por todo ello, el objeto que se persigue con la aprobación de esta nueva Ley de Protección de Datos Personales, es el de regular el tratamiento de los datos personales contenidos en los registros o bancos de datos de los organismos públicos. De esta forma, el derecho a la protección a terceros, como ya se ha dicho, es un derecho fundamental que debe ser respetado, que debe ser regulado y que puede convivir perfectamente con otros intereses, otros derechos, como en particular el derecho al acceso a la información pública, pero teniendo en cuenta que, en la transparencia administrativa, la administración de cristal no tiene por qué convertir al ciudadano en ciudadano de cristal.

Esta protección de los datos personales, su administración y transferencia, como se observará en el contenido del ordenamiento jurídico que se somete a consideración del Pleno de esta Soberanía, está vinculada a la observancia de ciertos principios reconocidos en el ámbito internacional. Dichos principios a los que nos referimos son los de: licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad.

Respecto del primero de dichos principios, debemos decir que, la licitud responde a la obligación que tienen las entidades públicas de tratar los datos personales únicamente para cumplir con las atribuciones legales que dichas entidades públicas tienen reconocidas. De esta forma, se advierte que los sistemas de datos, archivos o registros en poder de las entidades públicas no podrán utilizarse sino para los fines que la propia ley les confiere, con lo que, se garantiza que los datos de cualquier individuo no se emplearán con otros fines que pongan en peligro su intimidad.

Por cuanto hace al principio de consentimiento, en el proyecto de ley se refiere como una característica fundamental el que este consentimiento del titular, deba ser un consentimiento informado. Así el individuo debe conocer claramente la finalidad y el propósito del almacenamiento de sus datos y la posibilidad de que éstos sean dados a conocer a terceros. La autorización debe darse por escrito y la manera de revocarla es de la misma manera.

En relación a la calidad de los datos, la característica primordial de este principio es que, los datos que las entidades públicas recaben deban ser ciertos, adecuados, pertinentes y no excesivos, por lo que los sujetos encargados de la administración de dichos datos tienen la obligación de mantenerlos actualizados y verificar que éstos sean ciertos.

Respecto a los principios de confidencialidad y de seguridad, en relación al primero, consiste en que, de manera exclusiva, la persona interesada acceda a los datos personales o, en su caso, el responsable o el usuario del sistema de datos personales para su tratamiento, guardando el responsable del sistema como los usuarios, la secrecía debida, mientras que, por cuanto hace al principio de seguridad, éste busca garantizar que únicamente el responsable del sistema de datos personales o en su caso los usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales.

El sustento en la inclusión de estos principios es que, la cesión de datos, es decir su transmisión, a terceras personas, constituye un peligro ya que resulta complicado que el ciudadano pueda controlar de modo efectivo sus datos personales si la persona o la institución a la que se los ha proporcionado puede comunicarlos libremente a otros interesados.

Tal peligro se observa de modo relevante en la actuación de los poderes públicos ya que, con el progreso acelerado de las tecnologías de la información y en un escenario donde todas las administraciones apuestan por su informalización interna y externa, no es descabellado pensar en un mecanismo que permitiera conocer todos los datos que, relacionados con un individuo, obran en los expedientes de una

determinada entidad pública. Será fácil, por lo tanto, agrupar esas facetas de la personalidad que aisladamente consideradas, pueden carecer de significación intrínseca, pero que coherentemente enlazadas entre sí, arrojan un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Con base en los argumentos anteriormente esgrimidos, podemos inferir que “La dignidad de la persona y el libre desarrollo de la personalidad, son fundamento del orden político y de la paz social”.

Por último, los principios de disponibilidad y temporalidad hacen alusión a la posibilidad de que el almacenamiento de los datos personales almacenados permita al interesado el ejercicio de los derechos de acceso, rectificación, cancelación y oposición y que dichos datos deban ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados.

- 14.** Es muy importante que haya una autoridad única que de algún modo establezca criterios uniformes, porque si la legislación no es clara se puede producir una serie de discordancias en el ordenamiento interno que no es aconsejable, por lo menos de frente a lo que se le debe proporcionar a los ciudadanos. Por tal motivo, en el contenido de la propuesta de Ley que hoy se presenta, se otorga a la Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala, la facultad de ser ella, a través del Registro Estatal de Datos Personales, la que lleve la inscripción de los sistemas de datos que obren en poder de las entidades públicas. Dicho registro tendrá

facultades de inspección y se encargará de velar por el cumplimiento de las disposiciones de esta Ley.

15. Hoy, sin temor a equivocarnos, podemos señalar que desde el ámbito gubernamental, las entidades públicas ya tienen un manejo masivo de datos en manos del Estado, no sólo los estadísticos, probablemente también en la administración tributaria, en materia de derecho del consumidor, de datos financieros, de datos relacionados con la actividad electoral de los ciudadanos y ciudadanas y por supuesto, todos los datos referidos a la administración de justicia. Ese volumen de datos ya demuestra la necesidad de un derecho de protección de datos regulado vía legal y la única esperanza que se tiene es la de avanzar hasta la ocasión y la oportunidad de tener leyes que permitan desarrollar después una cultura de protección de datos. Ya no tenemos tiempo de desarrollar la cultura antes de la ley, démosle la oportunidad a la ley de crear la cultura.

16. En mérito de los argumentos vertidos, podemos hablar de la responsabilidad que tiene el gobierno de proteger los datos personales que los individuos le entregan con propósitos específicos, de forma que éste debe garantizar el ejercicio de los derechos individuales, proteger la intimidad y evitar que la información personal se haga pública.

Es menester tener en cuenta que la protección de este derecho salvaguarda la voluntad de mantener fuera del conocimiento público aspectos de la vida personal tales como la convivencia familiar, la conducta sexual y afectiva, las creencias religiosas, el patrimonio personal, entre otros.

De nada sirve haber reformado la Constitución federal y la propia del Estado de Tlaxcala, haber incluido una serie de nuevos derechos, haber dotado de jerarquía constitucional a un conjunto de tratados internacionales sobre derechos humanos con los cuales se amplía el ámbito de derechos y libertades fundamentales del individuo, si no se acompaña esa creación con una política estatal que permita el acceso a la justicia para hacer valer esos derechos.

Como lo refería Lasalle: “la Constitución no es una simple hoja de papel. Hay que hacerla funcionar dado que es cuerpo y alma. La Constitución es norma jurídica y, por ende, vinculante, exigible y alegable ante los tribunales”. Entonces, para hacer operable el derecho de protección de datos personales, deben existir las garantías que permitan su ejercicio en la práctica cotidiana.

En el contexto de la ineludible obligación del Estado de proporcionar medios jurídicos, se incrusta la razón de ser, de este nuevo ordenamiento legal, que surge como un “muro de contención” para evitar el abuso de las entidades públicas y demás sujetos obligados en el manejo de los sistemas de datos personales que administren con motivo de sus funciones.

Como conclusión de todos los argumentos, podemos decir que la protección de datos es un elemento fundamental de la sociedad de la igualdad. Es una condición esencial de la sociedad de la participación; es un instrumento necesario para salvaguardar la sociedad de la libertad y

un componente imprescindible de la sociedad de la dignidad, porque esto es esencial. La protección de datos es íntima relación con el respeto a la dignidad de las personas.

Por los razonamientos anteriormente expuestos, esta Comisión se permite someter a la consideración de esta Honorable Asamblea Legislativa la siguiente Iniciativa con Carácter de Dictamen con:

PROYECTO
DE
LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL ESTADO DE
TLAXCALA

TÍTULO PRIMERO
DISPOSICIONES GENERALES

CAPÍTULO ÚNICO
DEL OBJETO Y ÁMBITO DE APLICACIÓN

Artículo 1. La presente Ley es de orden público e interés general y tiene por objeto garantizar la protección de datos personales, que el sector público

recabe o posea para un uso posterior registrados en soporte físico o automatizado, regulando su tratamiento legítimo, controlado e informado, con la finalidad de garantizar la privacidad y proteger el derecho a la autodeterminación informativa de las personas; conforme a lo dispuesto en el segundo párrafo de los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos y en la fracción V del artículo 19 de la Constitución Política del Estado Libre y Soberano de Tlaxcala.

La administración de los datos personales en posesión de los particulares estará regulada por la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Artículo 2. Son sujetos obligados por esta ley:

- I. Los Poderes del Estado;
- II. Las dependencias centralizadas y las entidades paraestatales de la administración pública estatal;
- III. Los organismos públicos autónomos;
- IV. Los organismos públicos descentralizados, patronatos de la administración pública dependiente del Poder Ejecutivo del Estado;
- V. Los partidos políticos, asociaciones y agrupaciones políticas;
- VI. Los ayuntamientos, comisiones municipales, dependencias y entidades de la administración pública municipal, organismos públicos descentralizados municipales, las empresas de participación municipal, fideicomisos públicos municipales, así como las presidencias de comunidad y delegaciones municipales;

vii. Aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público.

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

Área Responsable del Sistema de Datos Personales: La unidad administrativa, receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de las entidades públicas, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida la Comisión.

Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por los sujetos obligados, a través del cual, de forma previa al tratamiento de sus datos personales, se le informa al interesado, los datos que de él se recaban y con qué fines.

Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Bloqueo de datos personales: La identificación y reserva de datos personales con el fin de impedir su tratamiento. Una vez transcurrido el periodo de bloqueo, procederá la cancelación de los datos en el sistema de datos personales.

Cancelación. Eliminación de determinados datos de un sistema de datos personales previo bloqueo de los mismos.

Cesión de datos personales: Toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros ficheros y la comunicación de

datos realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre sujetos obligados.

Cesionario. Persona física o moral, pública o privada, a la que un sujeto obligado realice una cesión de datos personales.

Comisión: La Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala.

Consentimiento: toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen.

Datos personales: La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable.

Datos personales sensibles: Aquellos datos personales que afecten 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 aquellos relativos al origen racial o étnico, características físicas, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, vida afectiva y familiar, afiliación sindical, opiniones políticas, preferencia sexual del individuo, patrimonio, domicilio, número telefónico, y en general, cualquier otra que afecten su intimidad.

Disociación: Procedimiento mediante el cual los datos personales que se obtengan no puedan asociarse a una persona física identificada o identificable, ni permitir por su estructura, contenido o grado de desagregación, la identificación del mismo.

Encargado: La persona física o jurídica, sea de orden público o privado, o servidor público, que sola o conjuntamente con otras, lleve a cabo el tratamiento físico o automatizado de los datos personales por cuenta del responsable.

Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado en el Reglamento de esta Ley.

Información confidencial: La información en poder de las entidades públicas, que contenga datos personales sensibles, protegida por el derecho fundamental a la privacidad conforme lo dispone esta Ley.

Información Pública: Todo registro, archivo o cualquier dato que se recopile, mantenga, procese o se encuentre en poder de los sujetos obligados a que se refiere esta Ley.

Interesado: Persona física, titular de los datos personales que sean objeto del tratamiento al que se refiere la presente Ley.

Ley: la Ley de Protección de Datos Personales para el Estado de Tlaxcala.

Reglamento: El Reglamento de la Ley de Protección de Datos Personales para el Estado de Tlaxcala.

Registro: El Registro Estatal de Protección de Datos Personales, que fungirá como un órgano técnico de la Comisión.

Responsable: Persona física designada por el Titular u órgano de gobierno del sujeto obligado, que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos.

Sistema de Datos Personales: El conjunto organizado de datos, archivos, registros, ficheros, bases o banco de datos personales de los sujetos obligados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Soporte físico. Es el medio de almacenamiento que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Es decir, documentos, oficios, formularios impresos, fotografías, placas radiológicas, carpetas, expedientes.

Soporte electrónico: Medio de almacenamiento que requieren aparatos con circuitos electrónicos como lo son las cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos CDs y DVDs, discos magneto-ópticos, discos magnéticos; para poder examinar, modificar o almacenar datos, (flexibles y duros).

Supresión: Eliminación de un sistema de datos personales mediante acuerdo publicado en el Periódico Oficial del Gobierno del Estado de Tlaxcala.

Sujeto Obligado: Aquellos a que se refiere el artículo 2 de esta Ley.

Tercero: La persona física o moral, nacional o extranjera, distinta del **interesado** o del responsable de los datos.

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones, efectuada mediante procedimientos de carácter automatizado o físico, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, interconexión o cualquier otra forma que permita obtener información

de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos.

Usuario. Aquel autorizado por el sujeto obligado para prestarle servicios para el tratamiento de datos personales.

Artículo 4. La interpretación de esta Ley se realizará conforme a lo previsto por la Constitución Política de los Estados Unidos Mexicanos, la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales respectivos.

En todo lo no previsto en los procedimientos a que se refiere esta Ley, se aplicará de manera supletoria la Ley del Procedimiento Administrativo del Estado de Tlaxcala y sus Municipios y el Código de Procedimientos Civiles del Estado Libre y Soberano de Tlaxcala.

TITULO SEGUNDO

DE LA TUTELA DE DATOS PERSONALES

CAPÍTULO I

DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Artículo 5. Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, estatal y municipal, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

Artículo 6. Los responsables de los sistemas de datos personales en posesión de las entidades públicas, deberán observar los principios siguientes:

Licitud: Consiste en que la posesión y tratamiento de sistemas de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada sujeto obligado y deberán obtenerse a través de medios previstos en dichas disposiciones.

Los sistemas de datos personales no pueden tener finalidades contrarias a las leyes o a la moral pública y en ningún caso pueden ser utilizados para finalidades distintas o incompatibles con aquella que motivaron su obtención. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Consentimiento: Consistente en que el tratamiento de datos personales debe estar sujeto a la manifestación de la voluntad libre, expresa, inequívoca, específica e informada, del interesado.

Calidad de los Datos: Consiste en que los datos personales recabados deben ser exactos, ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido y respecto a las

atribuciones legales del sujeto obligado que los posea.

Confidencialidad: Consistente en que, de manera exclusiva, la persona interesada acceda a los datos personales o, en su caso, el responsable o el usuario del sistema de datos personales para su tratamiento, guardando el responsable del sistema como los usuarios, la secrecía debida.

Atendiendo al principio de confidencialidad, los datos personales adquieren el carácter de irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del interesado.

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

Los instrumentos jurídicos relativos a la contratación de servicios del encargado del sistema de datos personales, así como de los usuarios, deberán prever la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, así como la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación y las sanciones a que se hagan acreedores quienes incumplan con el principio de confidencialidad. Lo anterior, sin perjuicio de las responsabilidades penales, civiles o administrativas previstas en otras disposiciones aplicables.

El responsable del sistema de datos personales o los usuarios podrán ser relevados del deber de confidencialidad por resolución judicial y cuando se anteponga la salud pública o la seguridad nacional, estatal o municipal.

Seguridad: Consiste en la adopción de medidas que garanticen, por parte del

responsable, la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Disponibilidad: Esto es que, los datos personales sean almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado.

Temporalidad: Consiste en que los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados, excepto que éstos sean tratados con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación.

Los datos personales que tengan fines históricos podrán ser conservados de manera íntegra y permanente.

CAPÍTULO II

DE LAS MEDIDAS DE SEGURIDAD

Artículo 7. Los sujetos obligados, establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integridad de cada archivo, sistema o base de datos personales que posean, con la finalidad de preservar el pleno ejercicio de los derechos tutelados en la presente Ley, frente a su alteración, pérdida, transmisión y acceso no autorizado, de conformidad al tipo de datos contenidos en dichos archivos, sistemas o bases de datos.

Dichas medidas se considerarán de naturaleza restringida, serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos

personales, deberán constar por escrito y ser comunicadas a la Comisión para su inscripción en el Registro.

Las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público o, en su caso, la persona física o moral que intervengan en el tratamiento de datos personales con el carácter de responsable del archivo o sistema de datos personales o usuario, según corresponda. Cuando se trate de usuarios se deberán incluir los datos del acto jurídico mediante el cual, el sujeto obligado otorgó el tratamiento del archivo o sistema de datos personales.

Artículo 8. Todos los servidores públicos o el personal involucrado en el tratamiento de datos personales, así como los usuarios, deberán observar las disposiciones contenidas en esta Ley así como en los lineamientos emitidos por la Comisión y demás normatividad aplicable para cada sistema de datos personales.

SECCIÓN PRIMERA

DE LOS TIPOS DE SEGURIDAD

Artículo 9. El sujeto obligado, responsable de la tutela y tratamiento del sistema de datos personales, adoptará los siguientes tipos de seguridad:

- I. Física. Relativa a las medidas tendentes a proteger y dar mantenimiento óptimo a las instalaciones, equipos, soportes o sistemas de datos, cuyo objeto sea la prevención de riesgos causados por casos fortuitos o causas de fuerza mayor;
- II. Lógica. Relativa a la autenticación de las personas o usuarios

autorizados para el tratamiento de datos personales, de acuerdo con su función;

- III. De comunicaciones y redes informáticas. Tiene por objeto establecer las restricciones preventivas o de riesgos que deberán observar los usuarios de sistemas de datos personales para acceder a dominios o instalar programas informáticos autorizados, así como para el manejo de telecomunicaciones;
- IV. De cifrado. Tiene por objeto la implementación de algoritmos, claves, contraseñas, así como los dispositivos concretos de protección que garanticen la integridad y confidencialidad de la información, y
- V. De desarrollo y Aplicaciones. Relativa a las autorizaciones requeridas para la creación o tratamiento de datos personales, para garantizar el adecuado desarrollo y uso de los mismos, previendo la participación de los usuarios, la separación de entornos, las consideraciones especiales relativas a las aplicaciones y las pruebas realizadas a éstas, la metodología a seguir y los ciclos de vida de los sistemas de datos.

SECCIÓN SEGUNDA

DE LOS NIVELES DE SEGURIDAD

Artículo 10. Además de los tipos de seguridad a que se refiere el artículo anterior, el responsable de la tutela y tratamiento del sistema de datos personales, adoptará y observará los siguientes niveles de seguridad:

- I. **Básico.-** El que comprende la elaboración de la normativa que contenga las medidas generales de seguridad cuya aplicación es obligatoria para

todos los sistemas de datos personales, mediante la emisión del Documento de Seguridad que habrán de observar todos los servidores públicos del sujeto obligado, así como para aquellas personas que con motivo de la prestación de un servicio, tengan acceso a los sistemas de datos personales o al sitio donde éstos se ubican. El documento de seguridad deberá contener, cuando menos:

- a) Nombre del sistema;
- b) Cargo y adscripción del responsable;
- c) Ámbito de aplicación;
- d) Estructura y descripción del Sistema de Datos Personales;
- e) Especificación detallada de la categoría de datos personales contenidos en el Sistema;
- f) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales. El titular u órgano de dirección del sujeto obligado, en coordinación con el responsable del Sistema de Datos Personales, adoptarán las medidas necesarias para que los servidores públicos del sujeto obligado conozcan las normas de seguridad y las responsabilidades y consecuencias en que se pudiera incurrir en caso de incumplimiento;
- g) Medidas, normas, procedimientos y criterios para garantizar el nivel de seguridad;
- h) Registro de incidencias. Para tal efecto se hará constar el momento y el tipo de incidencia ocurrida y se establecerán los procedimientos de notificación, gestión y respuesta;

- i) Identificación y autenticación de los usuarios, consistente en la obligación del responsable de adoptar medidas para que los encargados y usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. Para tal efecto, el responsable deberá mantener actualizada una relación de personas autorizadas y los accesos autorizados para cada una de ellas;
- j) Control de acceso, que implica que el responsable deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo por las personas autorizadas en el sistema de datos personales, así como la facultad del responsable de conceder, alterar o anular la autorización para el acceso a los sistemas de datos personales.
- k) Gestión de soportes, e
- l) Copias de respaldo y recuperación. Esto es, que en caso de que los datos personales se encuentren en soporte físico, se procurará que el respaldo se efectúe mediante la digitalización de los documentos, mientras que para soportes electrónicos se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental.

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

II. **Medio.-** Consiste en la adopción de aquellas medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos administrados con motivo de la comisión de infracciones administrativas o penales, por tratarse de asuntos de 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, considerará los siguientes aspectos:

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

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

b) Auditoría. Las medidas de seguridad implementadas para la protección de los sistemas de datos personales se someterán a una auditoría interna o externa, mediante la que se verifique el

cumplimiento de las disposiciones de esta Ley y demás procedimientos vigentes en materia de seguridad de datos, al menos, cada dos años.

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

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

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

- d) Pruebas con datos reales. Las pruebas que se lleven a cabo con efecto de verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación o modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se

asegure el nivel de seguridad correspondiente al tipo de datos tratados. Si se realizan pruebas con datos reales, se elaborará con anterioridad una copia de respaldo.

III. **Alto.-** Relativo a las medidas de seguridad aplicables a sistemas de datos concernientes a la 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) **Seguridad en la distribución de soportes.** La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión;

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

De cada acceso se guardarán, al menos, la identificación del usuario, la

fecha y hora en que se realizó, el sistema accedido, el tipo de acceso y si éste fue autorizado o denegado.

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

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

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

Artículo 11. Las medidas de seguridad a las que se refiere en el presente capítulo, constituyen mínimos exigibles, por lo que los sujetos obligados, podrán adoptar 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 serán consideradas confidenciales y únicamente se comunicará a la Comisión, a través del Registro, para su inscripción en el nivel de seguridad aplicable.

CAPÍTULO III

DE LA DENUNCIA

Artículo 12. Cualquier persona podrá presentar una denuncia ante la Comisión, solicitando una investigación con motivo de una probable violación a las disposiciones establecidas en esta Ley, siempre y cuando no se encuentre vinculada con el ejercicio de los derechos ARCO.

Toda denuncia presentada ante la Comisión, deberá cumplir cuando menos con los siguientes requisitos:

I. El nombre del denunciante o en su caso, la autoridad que promueve la denuncia;

II. En caso de que la denuncia sea presentada por el interesado, deberá aportar los documentos que acrediten su identidad;

III. Nombre del sujeto obligado que es denunciado;

IV. Descripción clara y precisa del acto o resolución que motiva la denuncia, especificando el artículo y, en su caso, la fracción de la Ley que se considera no fueron observados;

V. Las pruebas que tengan relación directa con el acto por el que se inconforma, y

VI. El domicilio del denunciante o correo electrónico para recibir notificaciones. En caso de que no se señale domicilio alguno, o bien se señala un domicilio fuera del Estado de Tlaxcala, las notificaciones se practicarán a través de los

estrados o a través de la página de internet de la Comisión, pudiendo el denunciante autorizar a terceras personas para recibir notificaciones y documentos en su nombre.

La Comisión deberá prevenir al denunciante de las deficiencias de forma y fondo que contenga su escrito de denuncia.

Artículo 13. Las denuncias que se reciban con motivo de infracciones contenidas en la presente Ley serán sustanciadas de conformidad con el procedimiento que para tal efecto apruebe la Comisión en un plazo no mayor de cuarenta días, contados a partir de la fecha en la que se tenga por recibida.

CAPÍTULO IV

DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 14. El tratamiento de los datos personales, requerirá el consentimiento inequívoco, expreso y por escrito del interesado.

Se entenderá que el consentimiento otorgado por el interesado es expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos; mientras que el consentimiento será tácito cuando habiéndose puesto a disposición del interesado el aviso de privacidad, éste no manifieste su oposición.

De manera previa al tratamiento de datos personales, los sujetos obligados deberán informar al interesado mediante la emisión del aviso de privacidad, que

los datos personales recabados serán incorporados, protegidos y tratados en el Sistema de Datos Personales del sujeto obligado, el fundamento legal que faculta al sujeto obligado para recabar los datos personales, la finalidad del tratamiento y los destinatarios del mismo así como sobre la posible cesión o transmisión de los datos personales que conforme a la ley, pueda realizarse. Asimismo se le indicará al interesado sobre la prohibición que tiene el sujeto obligado de difundir sus datos sin que mediare consentimiento expreso para ello, salvo las disposiciones previstas en esta Ley, sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y el cargo y dirección del responsable del sistema de datos personales y en su caso de los destinatarios.

El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

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

II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, la información a que se refiere el párrafo segundo del presente artículo, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Artículo 15. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del interesado, para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

El consentimiento a que se refiere el presente artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

Artículo 16. No se requerirá el consentimiento inequívoco, expreso y por escrito del interesado, en los casos y excepciones siguientes:

- I. Cuando se recaben para el ejercicio de las atribuciones legales conferidas a los sujetos obligados;
- II. Cuando exista una orden judicial;
- III. Cuando se refieran a las partes de un convenio de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;
- IV. Cuando el interesado no esté en posibilidad de otorgar su consentimiento por motivos de salud y el tratamiento de sus datos resulte necesario para la prevención o para el diagnóstico médico, la prestación o gestión de asistencia sanitaria o tratamientos médicos, siempre que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u

obligación equivalente;

- V. Cuando la transmisión se encuentre expresamente previsto en una ley;
- VI. Cuando la transmisión se produzca entre organismos gubernamentales y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos;
- VII. Cuando se den a conocer a terceros para la prestación de un servicio que responda al tratamiento de datos personales, mediante la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente que la comunicación de los datos será legítima en cuanto se limite a la finalidad que la justifique;
- VIII. Cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia, o para la realización de estudios epidemiológicos, y
- IX. Cuando los datos figuren en registros públicos en general y su tratamiento sea necesario siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Artículo 17. El sujeto obligado no podrá difundir o ceder los datos personales contenidos en los sistemas de datos desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso por escrito o por un medio de autenticación similar, del interesado a que haga referencia la información. Para tal efecto, el responsable contará con los formatos necesarios para recabar dicho consentimiento.

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

Artículo 18. Cuando por motivo de la utilización o cesión de los datos de carácter personal, se impida gravemente o se atente de igual modo contra el ejercicio de derechos de las personas, la Comisión podrá requerir a los responsables de los sistemas de datos personales, la suspensión en la utilización o cesión de los datos. Si el requerimiento fuera desatendido, mediante resolución fundada y motivada, la Comisión bloqueará tales sistemas, de conformidad con el procedimiento que al efecto se establezca. El incumplimiento a la inmovilización ordenada por la Comisión será sancionado por la autoridad competente de conformidad por la Ley de Responsabilidades de los Servidores Públicos para el Estado de Tlaxcala, con independencia de las sanciones que se establezcan en esta Ley y de las responsabilidades civiles y penales que deriven por esta omisión.

Artículo 19. El tratamiento de los sistemas de datos personales en materia de salud, se rige por lo dispuesto por la Ley de la materia y demás normas que de ella se deriven. El tratamiento y cesión de esta información obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera tal que se mantenga la confidencialidad de los mismos, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación científica, de salud pública o con fines judiciales, en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales. El acceso a los datos y documentos relacionados con la salud de las personas queda limitado estrictamente a los fines específicos de cada caso.

Artículo 20. Los sistemas de datos personales que hayan sido objeto de tratamiento, deberán ser suprimidos una vez que concluyan los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines por los cuales fueron recabados.

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

Artículo 21. Cuando en el sistema de datos personales, se recaben datos de menores de edad, el responsable del sistema de datos personales, deberá solicitar el consentimiento expreso de los padres del menor, o de quienes ejerzan sobre él la patria potestad o tutela. Para tal efecto, los responsables del sistema de datos personales, deberán establecer formatos con un lenguaje fácilmente comprensible para los menores.

No podrán recabarse datos sensibles del menor o aquellos que tengan por objeto obtener información sobre los miembros de su familia, como lo son los relativos a la ocupación, ingresos económicos, información patrimonial o cualquier otro dato sensible de sus padres o tutores; salvo aquellos que sean necesarios para recabar la autorización prevista en el párrafo anterior, tales como el nombre y domicilio de éstos.

Para efectos de lo dispuesto en este artículo, el responsable del sistema de datos personales del sujeto obligado, deberá adoptar las medidas y procedimientos necesarios para garantizar que se ha comprobado de manera

efectiva, la edad del menor y la autenticidad del consentimiento otorgado, en su caso, por los padres o de quien ejerza la patria potestad o tutela de éste.

CAPÍTULO V

DE LA CESIÓN Y TRANSFERENCIA DE DATOS PERSONALES

SECCIÓN PRIMERA

DE LA CESIÓN DE DATOS PERSONALES

Artículo 22. Los datos que obren en un sistema de datos personales sólo se pueden ceder a persona con interés legítimo, con el previo consentimiento del interesado, al que se debe informar suficientemente sobre la identidad del cesionario, y la finalidad de la cesión.

El consentimiento de la cesión es revocable, mediante notificación indubitable al responsable de los datos.

Artículo 23. La cesión no requiere el consentimiento del interesado, cuando:

- I. La ley no lo exija;
- II. La cesión se realice entre dependencias y organismos públicos en forma directa, en el ejercicio de sus atribuciones y en el ámbito de sus competencias;

- III. Por razones de interés social, de seguridad pública o estatal, o salud pública, y
- IV. Se aplique un procedimiento de disociación de datos de manera que no se puedan atribuir a persona identificada o identificable.

Artículo 24. El cesionario queda sujeto a las mismas obligaciones legales y reglamentadas del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el órgano de control y el interesado.

SECCIÓN SEGUNDA

DE LA TRANSFERENCIA DE DATOS PERSONALES

Artículo 25. La transferencia de datos con otros sujetos obligados, entidades federativas u otros países, procederá en los casos siguientes:

- I. Cuando dicha transferencia se encuentre prevista en una Ley o en un Tratado internacional ratificado por nuestro país;
- II. Por orden judicial;
- III. Intercambio de datos en materia de salud, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica;
- IV. Cuando la transferencia se acuerde en un convenio o instrumentos vigente en el que el Estado de Tlaxcala sea parte, y
- V. Cuando la transferencia tenga por objeto la cooperación nacional para la lucha contra el crimen organizado, el terrorismo, el narcotráfico y delitos contra la humanidad.

No podrán realizarse transferencias temporales ni definitivas de datos personales que hayan sido objeto de tratamiento, cuando los destinatarios de dicha información no proporcionen un nivel de seguridad y protección de datos personales equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en esta Ley se obtenga autorización previa de la Comisión.

El carácter adecuado del nivel de protección que ofrece el sujeto obligado o la entidad federativa de destino, se evaluará por la Comisión, atendiendo a todas las circunstancias que concurran en la transferencia de datos personales. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, la institución de origen y la institución pública destinataria de los datos personales, las normas de derecho, generales o sectoriales, vigentes en la entidad federativa de que se trate y las medidas de seguridad en vigor.

Artículo 26. En caso de que los destinatarios de los datos sean instituciones de otras entidades federativas, los sujetos obligados deberán asegurarse que tales instituciones garanticen que cuentan con niveles de protección, semejantes o superiores, a los establecidos en esta Ley y, en la propia normatividad del sujeto obligado. Cuando los destinatarios de los datos sean personas o instituciones de otros países, el responsable del sistema de datos personales deberá realizar la cesión de los mismos, conforme a las disposiciones previstas en la legislación federal aplicable, siempre y cuando se garanticen los niveles de seguridad y protección previstos en la presente Ley.

Artículo 27. En el procedimiento de transferencia de datos personales a otros países u organismos internacionales, se observará lo dispuesto por la legislación federal en la materia y se efectuará, por conducto de las autoridades federales competentes, según lo determine la Ley o lo estipulen los convenios de colaboración que nuestro país haya celebrado al respecto.

TÍTULO TERCERO

DE LOS SISTEMAS DE DATOS PERSONALES

CAPÍTULO I

DEL SISTEMA DE DATOS PERSONALES

EN POSESIÓN DE LOS SUJETOS OBLIGADOS

Artículo 28. La creación, modificación o supresión de los sistemas de datos personales, incumbe a cada sujeto obligado, de conformidad con la resolución emitida por su titular u órgano de gobierno correspondiente, conforme a su respectivo ámbito de competencia y observando lo dispuesto en la presente Ley y demás normatividad aplicable.

Para efectos de lo dispuesto en el párrafo anterior, la resolución que sea emitida por el sujeto obligado, deberá publicarse en el Periódico Oficial del Gobierno del Estado de Tlaxcala, previo aviso que dentro de los diez días anteriores a su publicación, se dé a la Comisión.

En ningún caso, el registro de datos puede tener un fin contrario a la ley o a la moral.

Artículo 29. Los sistemas de datos personales en posesión de sujetos obligados, deberán inscribirse en el Registro.

Artículo 30. El formato de inscripción de datos personales deberá contener, cuando menos, los siguientes requisitos:

- I. El nombre del sujeto obligado que posea el Sistema de Datos Personales, la fecha de publicación y demás datos de localización de la resolución de creación del sistema en el Periódico Oficial del Gobierno del Estado de Tlaxcala;
- II. Nombre del sistema de datos personales así como el nombre del programa o subprograma gubernamental para el que se generó dicho sistema;
- III. Número de registros por programa, sistema o base de datos;
- IV. Nombre y cargo del responsable así como el nombre de los usuarios;
- V. Domicilio, teléfono y correo electrónico del sujeto obligado y del responsable así como la normatividad aplicable al sistema de datos personales
- VI. Características y finalidad del sistema de datos personales;
- VII. Los usos previstos que se darán al sistema, así como el soporte en el que se encuentra la base de datos;
- VIII. Procedimiento para relacionar la información recabada y tratada;
- IX. Naturaleza de los datos personales contenidos en el sistema;

- X. Forma, tiempo y lugar de recolección y actualización de datos;
- XI. Destino de los datos personales y personas físicas o morales a las que pueden ser transmitidos o se les puede permitir su consulta;
- XII. Modo de interrelacionar la información registrada;
- XIII. Tiempo de conservación de los datos;
- XIV. Formas y procedimientos por los cuales las personas pueden ejercer su derecho de acceso, rectificación, cancelación u oposición de sus datos personales, y
- XV. Medidas y niveles de seguridad que resulten aplicables.

Artículo 31. La resolución de creación del sistema de datos personales en posesión de un sujeto obligado, deberá contener lo siguiente:

- I. La identificación del Sistema de Datos Personales, indicando su denominación y normativa aplicable;
- II. La finalidad de la base de datos personales y los usos previstos para la misma;
- III. La estructura básica del sistema de datos personales, señalando de manera detallada los datos de identificación que contenga así como los datos especialmente protegidos y la descripción de los tipos de datos que se incluyan en el mismo, el tipo de tratamiento empleado por el sistema, sea este físico o automatizado y, en su caso, los datos de carácter obligatorio y facultativo;

- IV. Las instancias responsables del tratamiento del sistema de datos personales de carácter público y el nombre y cargo del responsable;
- V. EL domicilio oficial de la unidad administrativa ante la que se podrán ejercer los derechos de acceso, rectificación, cancelación y oposición;
- VI. El origen de los datos, señalando si el grupo o grupos de personas sobre las que se pretenda obtener datos de carácter personal o que de forma obligatoria deban proporcionarlos son los propios interesados, sus representantes, el sujeto obligado, etcétera;
- VII. El procedimiento que se aplicará para la recolección de los datos de carácter personal, sea éste a través de formulario, Internet, transmisión electrónica, etcétera;
- VIII. Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a otras entidades federativas u otros países, y
- IX. Las medidas de seguridad, con indicación del nivel y tipo de seguridad que resulte exigible.

Artículo 32. Cuando ocurra alguna modificación que afecte la integración y tratamiento de un Sistema de Datos Personales, el sujeto obligado deberá emitir la resolución de modificación correspondiente, la que debe indicar las modificaciones producidas a cualquiera de las fracciones a que se refiere el artículo anterior.

El sujeto obligado deberá publicar en el Periódico Oficial del Gobierno del Estado de Tlaxcala, la resolución de modificación del Sistema de Datos Personales y, dentro de los cinco días posteriores a la publicación, notificará

dicha circunstancia a la Comisión para efectos de que dicha modificación sea inscrita en el Registro.

Artículo 33. En el caso de que con motivo de la conclusión de los plazos de conservación de datos personales establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines para los cuales fueron recabados, el sujeto obligado deberá emitir la resolución de supresión del sistema de datos personales correspondiente.

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

La resolución que suprima un sistema de datos personales deberá publicarse en el Periódico Oficial del Gobierno del Estado de Tlaxcala, cuando menos con cuarenta y cinco días hábiles previos a la supresión del sistema de que se trate, debiendo establecer el destino que vaya a darse a los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción, de conformidad con lo dispuesto por la Ley de Archivos del Estado de Tlaxcala.

No procederá la supresión de los sistemas de datos personales cuando exista una previsión expresa en una norma que exija su conservación.

No podrán ser suprimidos de un sistema de datos personales, aquellos datos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.

Artículo 34. Cuando los sujetos obligados recaben datos personales, deberán informar previamente a los interesados de forma expresa, precisa e inequívoca los siguientes elementos:

- I. La existencia de un sistema de datos personales, el tratamiento que se dé a éstos, la finalidad de su obtención y los destinatarios de la información;
- II. La identidad y dirección del responsable del sistema de datos personales o, en su caso, de su representante, de las instancias responsables del tratamiento del sistema de datos personales y en su caso de los destinatarios;
- III. El carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas;
- IV. Las consecuencias de la obtención de los datos personales o de la negativa a suministrarlos;
- V. La posibilidad para que los interesados puedan ejercitar los derechos de acceso, rectificación, cancelación u oposición;
- VI. La cesión de la que pueden ser objeto los datos personales;
- VII. Las disposiciones que se dicten para la supresión de los registros, sistemas o bases de datos personales, estableciendo el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción, y podrán ser excluidos del proceso de destrucción, aquellos datos personales con finalidades históricas o estadísticas, que previamente hayan sido sometidos al procedimiento de disociación;
- VIII. La posibilidad de que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate

de datos personales que por disposición de una Ley sean considerados públicos.

Artículo 35. Cuando para la obtención de los datos personales se utilicen cuestionarios u otros impresos, figurarán en éstos, en forma claramente legible, los elementos a que se refiere el artículo anterior.

Cuando los datos de carácter personal no hayan sido recabados directamente del interesado, éste deberá ser informado de manera expresa, precisa e inequívoca, por el responsable del sistema de datos personales, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las fracciones I, II y V del artículo anterior.

Se exceptúa de lo previsto en el presente artículo cuando alguna ley expresamente así lo estipule.

Asimismo, tampoco regirá lo dispuesto en el presente artículo cuando los datos personales procedan de fuentes accesibles al público en general.

Artículo 36. Sólo con el consentimiento expreso y por escrito del interesado, podrán ser objeto de tratamiento los datos de carácter personal, considerados como sensibles, tal y como son: el origen étnico o racial, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Quedan exceptuados de lo dispuesto en el párrafo anterior, los sistemas de datos personales a cargo de los partidos políticos, sindicatos, asociaciones,

fundaciones y otras entidades sin fines de lucro, por cuanto se refiere a los datos relativos a sus asociados o miembros, sin perjuicio de que en el sistema de dichos datos personales se precise de la existencia del consentimiento previo del interesado.

Artículo 37. Queda prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar los datos personales señalados en el párrafo primero del artículo anterior y sólo pueden ser tratados cuando medien razones de interés general, así lo disponga una ley, lo consienta expresamente el interesado o, con fines estadísticos o históricos, siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

No obstante lo dispuesto en el párrafo primero del artículo anterior, los datos de carácter personal podrán ser objeto de tratamiento cuando éste resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional de la salud sujeto al secreto profesional.

Los datos personales sólo pueden ser utilizados para los fines que motivaron su obtención, o para fines compatibles con éstos.

Los datos personales objeto de tratamiento deben ser exactos y actualizados de manera que sean congruentes con los concernientes al interesado.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Las clínicas, hospitales, centros de salud y demás instituciones pertenecientes a la Secretaría de Salud del Estado, podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la Ley de Salud del Estado de Tlaxcala. Para tal efecto, en los estudios científicos o de salud pública, no será necesario el procedimiento de disociación previsto en esta Ley.

Los datos personales no incluidos, incompletos, inexactos o que estén en desacuerdo con la realidad de los que corresponden a la persona que conciernen, deben ser incluidos, complementados, actualizados, rectificados o cancelados, según corresponda.

Los datos personales deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación u oposición por parte del interesado.

Los sistemas de datos personales que hayan sido objeto de tratamiento, deberán ser suprimidos una vez que concluyan los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines para los cuales fueron recabados.

En el caso de que el tratamiento de los sistemas de bases de datos haya sido realizado por una persona distinta al sujeto obligado, el instrumento jurídico que dio origen al mismo deberá establecer la obligación de que el tratamiento de datos personales se realice conforme a las instrucciones del responsable del sujeto obligado, que estos datos no se aplicarán con fines distintos a los pactados en el instrumento jurídico, las medidas y niveles de seguridad que se implementen, las sanciones en caso de incumplimiento y el plazo de conservación por el usuario, al término del cual los datos deberán ser devueltos

en su totalidad al sujeto obligado, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

Artículo 38. Los archivos o sistemas creados con fines administrativos por las dependencias, instituciones o cuerpos de seguridad pública, en los que se contengan datos de carácter personal, quedarán sujetos al régimen general de protección previsto en la presente Ley.

Los datos de carácter personal obtenidos para fines policiales, podrán ser recabados sin consentimiento de las personas a las que se refieren, pero estarán limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención o persecución de delitos, debiendo ser almacenados en sistemas específicos, establecidos al efecto, que deberán clasificarse por categorías en función de su grado de confiabilidad.

La obtención y tratamiento de los datos a los que se refiere el presente artículo, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales.

Los datos personales recabados con fines policiales se cancelarán cuando no sean necesarios para las investigaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del interesado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial

firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 39. Los responsables de los sistemas de datos personales con fines policiales, para la prevención de conductas delictivas o en materia tributaria, podrán negar el acceso, rectificación, oposición y cancelación de datos personales en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, así como cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones.

CAPÍTULO II

DE LOS SUJETOS OBLIGADOS

Artículo 40. El titular o el órgano de gobierno de cada sujeto obligado, según corresponda, designará a un responsable de los sistemas de datos personales.

El titular del sujeto obligado será el responsable de decidir sobre la finalidad, contenido y uso del tratamiento del sistema de datos personales, quien podrá delegar dicha atribución en la unidad administrativa en la que se concrete la competencia material, a cuyo ejercicio sirva instrumentalmente el sistema de datos personales al cual esté adscrito el responsable del mismo.

Artículo 41. Los sujetos obligados serán responsables de la protección de los datos personales y, en relación con éstos, deberán:

I. Establecer mecanismos y procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, 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 los lineamientos que al respecto establezca la Comisión;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. Observar los principios establecidos en la presente Ley;

IV. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado;

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

VI. Garantizar que a partir del momento en el cual se recaben datos personales, se ponga a disposición de los individuos, el aviso de privacidad en el que se establezcan los propósitos para su tratamiento;

VII. Permitir, a través del responsable, en todo momento al titular de la información el ejercicio del derecho a conocer sobre sus datos personales, a solicitar su corrección o cancelación, así como a oponerse en los términos de esta ley, a que los mismos sean cedidos;

VIII. Rectificar o completar, de oficio, los datos personales que fueren inexactos o incompletos, en el momento en que tengan conocimiento de esta situación;

IX. Cancelar los datos personales cuando éstos dejen de ser necesarios para la finalidad para la cual se obtuvieron;

X. Elaborar y presentar a la Comisión, un informe correspondiente al cumplimiento de las obligaciones previstas en la presente Ley;

XI. Elaborar un plan de capacitación en materia de datos personales;

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

XIII. Proporcionar a la Comisión, por medio del responsable, la información necesaria para la protección de los derechos de acceso, rectificación, cancelación y oposición, y

XIV. Las demás que se deriven de la presente Ley.

Artículo 42. El responsable del sistema de datos personales, tendrá las siguientes facultades:

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

- II. Elaborar para su aprobación por el órgano de dirección de cada sujeto obligado, el informe correspondiente sobre las obligaciones previstas en la presente Ley, para efectos de ser presentado ante la Comisión a más tardar el último día hábil del mes de enero de cada año. La omisión de dicho informe será motivo de responsabilidad;
- III. Informar al interesado al momento de recabar sus datos personales, sobre la existencia y finalidad de los sistemas de datos personales, así como el carácter obligatorio o potestativo de proporcionarlos y las consecuencias de ello;
- IV. Adoptar los procedimientos adecuados para dar trámite a las solicitudes de informes, acceso, rectificación, cancelación y oposición de datos personales y, en su caso, para la cesión de los mismos; debiendo capacitar a los servidores públicos encargados de su atención y seguimiento;
- V. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;
- VI. Permitir en todo momento al interesado el ejercicio del derecho de acceso a sus datos personales, a solicitar la rectificación o cancelación, así como a oponerse al tratamiento de los mismos en los términos de esta Ley;
- VII. Actualizar los datos personales cuando haya lugar, debiendo corregir o completar de oficio o a petición del interesado, aquellos que fueren inexactos o incompletos, a efecto de que coincidan con los datos presentes de éste, siempre y cuando se cuente con el documento que avale la actualización de dichos datos;

- VIII. Guardar el secreto profesional respecto de los datos personales que obren en poder del sujeto obligado ;
- IX. Recibir la capacitación permanente y actualizada en materia de seguridad de datos personales;
- X. Emitir el proyecto de resolución respecto del ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos de las personas;
- XI. Llevar a cabo o, en su caso, coordinar la ejecución material de las diferentes operaciones y procedimientos en que consista el tratamiento de datos y sistemas de datos de carácter personal a su cargo;
- XII. Coordinar y supervisar la adopción de las medidas de seguridad a que se encuentren sometidos los sistemas de datos personales de acuerdo con lo dispuesto por la presente Ley y demás disposiciones legales aplicables;
- XIII. Fomentar al interior del sujeto obligado, la protección de datos personales, y
- XIV. Las demás que se deriven de la presente Ley o demás ordenamientos jurídicos aplicables.

Artículo 43. El responsable del sistema de datos personales tiene prohibido formular juicios de valor, que tengan como consecuencia directa el atentar contra el principio de confidencialidad, sobre los datos personales que trate de

forma automatizada, así como registrarlos cuando no se reúnan las condiciones técnicas de integridad o seguridad.

Además de lo dispuesto en el párrafo anterior, el responsable del sistema de datos personales, así como quienes intervengan en la colecta y el tratamiento de los datos personales, están obligados a guardar el secreto profesional, incluso aún después de que concluyan sus relaciones con el interesado.

Artículo 44. El responsable no estará obligado a cancelar los datos personales cuando:

- I. Se refiera a las partes de un documento oficial y sean necesarios para su desarrollo y cumplimiento;
- II. Deban ser tratados por disposición legal;
- III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;
- IV. Sean necesarios para proteger los intereses jurídicamente tutelados del interesado;
- V. Sean necesarios para realizar una acción en función del interés público;
- VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el interesado, y
- VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto al secreto profesional.

El interesado tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al interesado.

Artículo 45. El sujeto obligado no podrá difundir o ceder los datos personales contenidos en los archivos, sistemas o bases de datos personales desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso por escrito o por un medio de autenticación similar, de las personas a que haga referencia la información. Al efecto, el Área Responsable del Sistema de Datos Personales, contará con los formatos necesarios para recabar dicho consentimiento.

TÍTULO CUARTO

DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO I

DE LA COMISIÓN DE ACCESO A LA INFORMACIÓN

PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

DEL ESTADO DE TLAXCALA

Artículo 46. La Comisión, es el órgano encargado de dirigir y vigilar el cumplimiento de la presente Ley, así como de las normas que de ella deriven; será la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales.

Artículo 47. La Comisión tendrá las atribuciones siguientes:

- I. Establecer, en el ámbito de su competencia, las normas, criterios, lineamientos y políticas de observancia general, para la administración, seguridad y tratamiento de los datos personales en posesión de los sujetos obligados, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta Ley;
- II. Divulgar estándares y mejores prácticas nacionales e internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;
- III. Diseñar y aprobar los formatos de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;
- IV. Establecer sistemas electrónicos para la recepción y trámite de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;
- V. Llevar a cabo la inscripción de los sistemas de datos personales en posesión de los sujetos obligados;
- VI. Elaborar y mantener actualizado el registro del nivel de seguridad aplicable a los sistemas de datos personales, en posesión de los sujetos obligados, en términos de esta Ley;
- VII. Emitir opiniones sobre temas relacionados con la presente Ley, así como formular observaciones y recomendaciones a los sujetos

obligados, derivadas del incumplimiento de los principios que rigen esta Ley;

- VIII. Hacer del conocimiento del órgano de control interno del sujeto obligado que corresponda, las resoluciones que emita, relacionadas con la probable violación a las disposiciones materia de la presente Ley;
- IX. Orientar y asesorar a las personas que lo requieran acerca del contenido y alcance de los derechos que esta Ley les reconoce;
- X. Elaborar y publicar estudios e investigaciones, así como organizar seminarios, cursos, talleres y demás actividades que promuevan el conocimiento de la presente Ley y los derechos en relación a la protección de datos personales;
- XI. Solicitar y evaluar los informes presentados por los sujetos obligados respecto del ejercicio de los derechos previstos en esta Ley. Dicha evaluación se incluirá en el informe que la Comisión, a través del Comisionado Presidente deba rendir de forma anual al Congreso del Estado;
- XII. Establecer programas de capacitación en materia de protección de datos personales y promover acciones que faciliten a las entidades públicas y a su personal, participar de estas actividades, a fin de garantizar el adecuado cumplimiento de los principios que rigen la presente Ley;
- XIII. Promover entre las instituciones educativas, públicas y privadas, la inclusión dentro de sus actividades académicas curriculares y extracurriculares, los temas que ponderen la importancia del derecho a la protección de datos personales;
- XIV. Investigar, substanciar y resolver el recurso de revisión en los términos previstos en esta Ley;
- XV. Evaluar la actuación de las entidades públicas, mediante la práctica de

visitas de inspección periódicas de oficio, a efecto de verificar la observancia de los principios contenidos en esta Ley, las cuales en ningún caso podrán referirse a información de acceso restringido de conformidad con la legislación aplicable;

- XVI. Procurar la conciliación de los intereses de los interesados con los de las entidades públicas, cuando éstos entren en conflicto con motivo de la aplicación de la presente Ley;
- XVII. Promover y, en su caso, ejecutar la capacitación de los servidores públicos en materia de protección de datos personales;
- XVIII. Difundir entre los servidores públicos y los particulares, los beneficios de la protección de los datos personales, como también sus responsabilidades en el buen uso y conservación de los documentos que los contengan;
- XIX. Promover la elaboración de guías que expliquen los procedimientos y trámites materia de esta Ley;
- XX. Cooperar respecto de la materia de protección de datos con los demás sujetos obligados, las entidades federativas, los municipios, o sus órganos de protección de datos personales, mediante la celebración de acuerdos o programas, y
- XXI. Las demás que establezca esta Ley, y demás ordenamientos aplicables.

Artículo 48. A efecto de impulsar una cultura de protección de datos personales, se deberá promover el desarrollo de eventos que fomenten la profesionalización de los servidores públicos al servicio de los poderes del Estado y de los municipios, sobre los sistemas y las medidas de seguridad que precisa la tutela de los datos personales de cada sujeto obligado.

CAPÍTULO II
DEL REGISTRO ESTATAL DE PROTECCIÓN
DE DATOS PERSONALES

Artículo 49. El Registro Estatal de Protección de Datos Personales, es un órgano técnico de la Comisión, cuyo objeto primordial es llevar el control de los sistemas de datos personales inscritos ante la Comisión.

Artículo 50. Serán objeto de inscripción en el Registro Estatal de Protección de Datos Personales:

- I. Los sistemas de datos personales administrados por los sujetos obligados;
- II. Las actualizaciones que a dichos sistemas de datos personales, realicen los responsables de los sujetos obligados, y
- III. Los datos relativos a los sistemas de datos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

La información contenida en los sistemas de datos personales administrados por las entidades públicas, deberán actualizarse durante el primer trimestre de cada año, dentro del término que para tal efecto la Comisión determine.

Artículo 51. Los sistemas de datos personales en posesión de los sujetos obligados, deberán inscribirse en el Registro, debiendo contener la información a que se refiere el artículo 30 de esta Ley.

Cualquiera modificación a la información contenida en el Registro debe ser comunicada por el responsable, en términos de lo dispuesto por el artículo 32 de esta Ley, siendo motivo de sanciones previstas en esta Ley, el incumplimiento a lo dispuesto en este capítulo.

Artículo 52. El Registro estará presidido por el Comisionado que designe el Pleno del Consejo General de la Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala, quien fungirá como responsable del mismo y contará con el personal que la Comisión determine, de acuerdo a su capacidad presupuestaria, que sea necesario para el cumplimiento de las atribuciones en materia de inscripción, protección, control y vigilancia de los sistemas de datos personales.

Artículo 53. La Comisión, a través del Registro, podrá inspeccionar los sistemas de datos personales a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

Para tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

El personal del Registro que ejerza la inspección a que se refiere el párrafo anterior, estará obligado a guardar secreto sobre las informaciones que conozca en el ejercicio de sus funciones, incluso después de haber cesado en las mismas.

TÍTULO QUINTO

DE LOS DERECHOS Y DEL PROCEDIMIENTO PARA SU EJERCICIO

CAPÍTULO I

DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN

Y OPOSICIÓN DE DATOS PERSONALES

Artículo 54. Cualquier interesado, o su representante legal, en su caso, previa identificación mediante documento oficial, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos personales administrados por los sujetos obligados, siendo derechos independientes, de tal forma que no puede entenderse que el ejercicio de alguno de ellos sea requisito previo o impida el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

La respuesta a cualquiera de los derechos previstos en la presente ley, deberá ser proporcionada en forma legible e inteligible, pudiendo suministrarse, a opción del interesado, por escrito o mediante consulta directa.

Artículo 55. El derecho de acceso se ejercerá para solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevén hacer, en términos de lo dispuesto por esta Ley.

Artículo 56. Procederá el derecho de rectificación de datos del interesado, en los sistemas de datos personales, cuando el interesado demuestre de forma fehaciente con los medios de prueba idóneos, que tales datos son inexactos o incompletos, inadecuados o excesivos, siempre y cuando resulte notoriamente improcedente dicha rectificación.

No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos.

Artículo 57. El derecho de cancelación es la prerrogativa del interesado a solicitar que se eliminen los datos que resulten inadecuados o excesivos en el sistema de datos personales de que se trate, sin perjuicio de la obligación de bloquear los datos conforme a lo dispuesto por la Ley.

El interesado tendrá derecho a solicitar la cancelación de sus datos cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en los lineamientos emitidos por la Comisión, o cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente

a disposición de los sujetos obligados, para la atención de las posibles responsabilidades nacidas del tratamiento indebido, durante el plazo de prescripción de éstas. Cumplido el plazo deberá procederse a su supresión, en términos de la normatividad aplicable.

La supresión de datos no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos.

Cuando los datos personales del interesado hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer del conocimiento de quienes se encuentren tratando dichos datos personales, la solicitud de rectificación o cancelación, para que estos últimos procedan a efectuarla también.

Artículo 58. El interesado tendrá derecho a oponerse al tratamiento de sus datos personales, siempre que dichos datos hayan sido recabados sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario. De actualizarse tal supuesto, el responsable del sistema de datos personales deberá cancelar los datos relativos al interesado.

Artículo 59. Si los datos rectificadas o cancelados hubieran sido transmitidos previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan transmitido, en el caso de que se mantenga el tratamiento por este último, quién deberá también proceder a la rectificación o cancelación de los mismos.

CAPÍTULO II

DEL PROCEDIMIENTO

Artículo 60. La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que se formule a los sujetos obligados, se sujetarán al procedimiento establecido en el presente capítulo.

Artículo 61. La solicitud de acceso, rectificación, cancelación u oposición de datos personales, podrá realizarse en cualquiera de las siguientes modalidades:

- I. Por escrito, será la presentada personalmente por el interesado o su representante legal en el Área Responsable del Sistema de Datos Personales del sujeto obligado, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;
- II. Por comparecencia, cuando el interesado o su representante legal acuda directamente en la oficina del Área Responsable del Sistema de Datos Personales del sujeto obligado, a presentar de manera oral su solicitud, la cual deberá ser capturada en el formato respectivo;
- III. Por correo electrónico, en el caso de que el sujeto obligado cuente con mecanismos electrónicos que permitan la presentación de la solicitud por esta vía. ;
- IV. Por el sistema electrónico que la Comisión establezca para tal efecto, y

- v. Por vía telefónica, en términos de los lineamientos que expida la Comisión.

Artículo 62. La solicitud de acceso, rectificación, cancelación u oposición de los datos personales deberá contener, cuando menos, los requisitos siguientes:

- I. Nombre del sujeto obligado ante quien se promueve;
- II. Nombre completo del interesado, en su caso, el de su representante legal, así como los documentos que acrediten la identidad del interesado o de su representante legal;
- III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;
- IV. Cualquier otro elemento que facilite su localización;
- v. El domicilio, o correo electrónico para recibir notificaciones, y
- vi. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas.

Sin perjuicio de lo que dispongan otras leyes, sólo el interesado o su representante legal, previa acreditación de su identidad, podrán solicitar al sujeto obligado, a través del Área Responsable del Sistema de Datos Personales, que le permita el acceso, rectificación, cancelación o haga efectivo su derecho de oposición, respecto de los datos personales que le conciernan y que obren en un sistema de datos personales administrado por el sujeto obligado.

Cuando el procedimiento de acceso, rectificación, cancelación u oposición de datos personales se presente ante un sujeto obligado, el Área Responsable del Sistema de Datos Personales deberá notificar al interesado en el domicilio o medio electrónico señalado para tales efectos, en un plazo máximo de quince días hábiles contados desde la presentación de la solicitud, la determinación adoptada en relación con su solicitud, a efecto que, de resultar procedente, se haga efectiva la misma dentro de los diez días hábiles siguientes a la fecha de la citada notificación.

El plazo de quince días, referido en el primer párrafo de este artículo, podrá ser ampliado por única vez, por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Si al ser presentada la solicitud, se advierte que ésta no es precisa o no contiene todos los datos requeridos, en ese momento el sujeto obligado, en caso de ser solicitud verbal, deberá ayudar al solicitante a subsanar las deficiencias. Si los detalles proporcionados por el interesado no bastan para localizar los datos personales o son erróneos, el Área Responsable del Sistema de Datos Personales del sujeto obligado podrá prevenirlo, por una sola vez y, dentro de los cinco días hábiles siguientes a la presentación de la solicitud, para que aclare o complete su solicitud, apercibido de que de no desahogar la prevención se tendrá por no presentada la solicitud.

Este requerimiento interrumpe los plazos establecidos en los dos párrafos anteriores.

En el supuesto que los datos personales a que se refiere la solicitud obren en los sistemas de datos personales del sujeto obligado y éste considere improcedente la solicitud de acceso, rectificación, cancelación u oposición, se deberá emitir una resolución fundada y motivada al respecto. Dicha respuesta

deberá estar firmada por el responsable del sistema de datos personales del sujeto obligado.

Cuando los datos personales respecto de los cuales se ejerciten los derechos de acceso, rectificación, cancelación u oposición, no sean localizados en los sistemas de datos del sujeto obligado, se hará del conocimiento del interesado a través de acta circunstanciada, en la que se indiquen los sistemas de datos personales en los que se realizó la búsqueda. Dicha acta deberá estar firmada por un representante del órgano de control interno y el responsable del sistema de datos personales del sujeto obligado.

Artículo 63. La solicitud de acceso, rectificación, cancelación u oposición de datos personales, podrá realizarse en cualquiera de las siguientes modalidades:

- I. Por escrito, será la presentada personalmente por el interesado o su representante legal en el Área Responsable del Sistema de Datos Personales del sujeto obligado, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;
- II. Por comparecencia, cuando el interesado o su representante legal acuda directamente en la oficina del Área Responsable del Sistema de Datos Personales del sujeto obligado, a presentar de manera oral su solicitud, la cual deberá ser capturada en el formato respectivo;
- III. Por correo electrónico, en el caso de que el sujeto obligado cuente con mecanismos electrónicos que permitan la presentación de la solicitud por esta vía. ;
- IV. Por el sistema electrónico que la Comisión establezca para tal efecto, y

- v. Por vía telefónica, en términos de los lineamientos que expida la Comisión.

Artículo 64. La solicitud de acceso, rectificación, cancelación u oposición de los datos personales deberá contener, cuando menos, los requisitos siguientes:

- I. Nombre del sujeto obligado ante quien se promueve;
- II. Nombre completo del interesado, en su caso, el de su representante legal, así como los documentos que acrediten la identidad del interesado o de su representante legal;
- III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;
- IV. Cualquier otro elemento que facilite su localización, y
- V. El domicilio, o correo electrónico para recibir notificaciones.

Cuando se trate del derecho de acceso a los datos personales del interesado, éste deberá señalar la modalidad en la que prefiere se otorgue dicho acceso, la cual podrá ser consulta directa, copias simples o certificadas.

Tratándose del derecho de rectificación de datos, además de los requisitos previstos en este artículo, el interesado deberá indicar qué datos se requiere sean rectificadas o completadas acompañando la documentación que sustente dicha acción.

En la solicitud de cancelación, el interesado deberá indicar de manera precisa qué datos solicita que sean cancelados, aportando, en su caso, la

documentación que justifique las razones por las cuales considera que el tratamiento no se ajusta a lo dispuesto en esta Ley o en otras disposiciones legales.

Cuando la solicitud presentada ante el sujeto obligado se refiera al ejercicio del derecho de oposición del interesado respecto de sus datos personales, éste deberá señalar las razones por las cuales considera que el tratamiento de los datos no se ajusta a lo dispuesto en la Ley, o en su caso, acreditar la procedencia del ejercicio de su derecho.

En el caso de solicitudes de rectificación de datos personales, el interesado deberá indicar el dato que es erróneo y la corrección que debe realizarse y acompañar la documentación probatoria que sustente su petición, salvo que la misma dependa exclusivamente del consentimiento del interesado y ésta sea procedente.

En el caso de solicitudes de cancelación de datos personales, el interesado deberá señalar las razones por las cuales considera que el tratamiento de los datos no se ajusta a lo dispuesto en la Ley, o en su caso, acreditar la procedencia del ejercicio de su derecho de oposición.

El único medio por el cual el interesado podrá recibir la información referente a los datos personales será el Área Responsable del Sistema de Datos Personales, y sin mayor formalidad que la de acreditar su identidad y cubrir los costos de conformidad con la presente Ley y el Código Financiero para el Estado de Tlaxcala y sus Municipios.

Artículo 65. Presentada la solicitud de acceso, rectificación, cancelación u

oposición de datos personales, el área Responsable del Sistema de Datos Personales del Sujeto Obligado, observará el siguiente procedimiento:

- I. Procederá a la recepción y registro de la solicitud y devolverá al interesado, una copia de la solicitud registrada, que servirá de acuse de recibo, en la que deberá aparecer sello institucional, la hora y la fecha del registro;
- II. Registrada la solicitud, se verificará si cumple con los requisitos establecidos por el artículo anterior;
- III. Si la solicitud no es precisa o no contiene todos los datos requeridos, en ese momento el responsable del sistema de datos personales del sujeto obligado, en caso de ser solicitud verbal, ayudará al solicitante a subsanar las deficiencias. Si los detalles proporcionados por el solicitante no bastan para localizar los datos personales o son erróneos, el responsable podrá prevenir, por una sola vez y, dentro de los cinco días siguientes a la presentación de la solicitud, para que aclare o complete su solicitud, apercibido de que de no desahogar la prevención se tendrá por no presentada la solicitud;
- IV. Cuando del análisis realizado por el responsable respecto del contenido de una solicitud de acceso, rectificación, cancelación u oposición de datos personales, se desprenda que dicha solicitud corresponde a otra modalidad, se orientará al interesado para que presente su solicitud en la modalidad correspondiente, dentro de los cinco días siguientes a la recepción de la misma;
- V. Si la solicitud presentada no corresponde a una solicitud de acceso,

rectificación, cancelación u oposición sobre datos de carácter personal, el responsable deberá notificar dicha circunstancia al interesado dentro del plazo de cinco días siguientes a la recepción de la misma y, en su caso, orientarlo para que presente una solicitud de información pública o realice el trámite que corresponda;

- vi. En caso de que el sujeto obligado al que fue dirigida la solicitud de acceso, rectificación, cancelación u oposición, no sea el competente para atenderla, o que no corresponda al ámbito de sus atribuciones, dentro de los cinco días hábiles siguientes a aquel en que se tenga por presentada la solicitud, procederá a orientar al interesado o su representante legal, en el domicilio o medio señalado para recibir notificaciones, para que acuda al o los sujetos obligados que deban contar con los datos objeto del ejercicio de los derechos mencionados;
- vii. De cumplir con los requisitos, se turnará a la unidad administrativa que corresponda para que proceda a la localización de la información solicitada, a fin de emitir el acuerdo que corresponda;
- viii. La unidad administrativa informará al Área Responsable del Sistema de Datos Personales, de la existencia de la información solicitada. En caso de inexistencia, se procederá de conformidad con lo previsto por el artículo 60 para que el Área Responsable del Sistema de Datos Personales a su vez realice una nueva búsqueda en otra área o unidad administrativa;
- ix. Con la información a que se refiere la fracción anterior, el sujeto obligado procederá a emitir la resolución que recaiga a la solicitud de acceso, rectificación, cancelación u oposición de datos personales. El término para la emisión de dicha resolución no deberá exceder de

quince días hábiles contados a partir del día siguiente al de la fecha de presentación de la solicitud.

- x. El Área Responsable del Sistema de Datos Personales, notificará al interesado en el domicilio o a través del medio señalado para tal efecto, sobre la resolución emitida por el sujeto obligado, para efecto de que, si dicha solicitud resulta procedente, se haga efectiva la misma dentro de los quince días hábiles siguientes a la fecha en que sea notificada la resolución. Tratándose de solicitudes de acceso a datos personales, procederá el acceso, previa acreditación de la identidad del solicitante o de su representante legal, según corresponda.

En la resolución emitida por el sujeto obligado, se señalará el costo que por concepto de reproducción deberá pagar el solicitante en los términos del Código Financiero para el Estado de Tlaxcala y sus Municipios;

- xii. En cualquier caso, la entrega en soporte impreso o el acceso electrónico directo a la información solicitada se realizará de forma personal al interesado o a su representante legal, previa exhibición del original del documento con el que el interesado o su representante legal acreditó su identidad, y
- xii. De resultar procedente la rectificación, cancelación u oposición de los datos personales, el sujeto obligado deberá notificar al interesado dicha circunstancia, para que, dentro de los diez días siguientes, el interesado o su representante legal acrediten fehacientemente su identidad ante el responsable del sistema de datos personales y se proceda a realizar la rectificación, cancelación u oposición de los datos personales, según corresponda.

Los plazos referidos en el presente artículo, se podrán prorrogar por única vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Artículo 66. La obligación del sujeto obligado respecto del derecho de acceso, se dará por cumplida cuando se pongan a disposición de éste, los datos personales, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio que determine el Área Responsable del Sistema de Datos Personales, o bien, cuando se lleve a cabo la rectificación, cancelación u oposición de los datos personales, a que se refiere el artículo anterior.

Artículo 67. El interesado podrá recibir notificaciones en el domicilio que haya señalado para tal fin, vía correo electrónico o correo certificado o en los estrados del Área Responsable de los Sistemas de Datos Personales del sujeto obligado.

En el caso de que el solicitante no señale domicilio o algún medio de los autorizados por esta ley para oír y recibir notificaciones, todo tipo de notificaciones, incluso las personales se realizará por lista que se fije en los estrados del Área Responsable del Sistema de Datos Personales del sujeto obligado que corresponda o de la Comisión, según sea el caso.

En el caso de solicitudes de acceso a datos personales, el interesado o, en su caso, su representante legal deberá acreditar su identidad y personalidad al momento de la entrega de la información. Asimismo, deberá acreditarse la identidad antes de que el sujeto obligado proceda a la rectificación o cancelación.

El único medio por el cual el interesado podrá recibir la información referente a

los datos personales será el Área Responsable del Sistema de Datos Personales del sujeto obligado y sin mayor formalidad que la de acreditar su identidad y cubrir los costos de conformidad con el Código Financiero para el Estado de Tlaxcala y sus Municipios.

Artículo 68. El trámite de solicitud de acceso, rectificación, cancelación u oposición de datos personales es gratuito. No obstante, el interesado deberá cubrir los costos de reproducción de los datos solicitados, en términos de lo previsto por el Código Financiero para el Estado de Tlaxcala y sus Municipios.

Los costos de reproducción de la información solicitada se cobrarán al solicitante de manera previa a su entrega y se calculará atendiendo a:

- I. El costo de los materiales utilizados en la reproducción de la información;
- II. El costo de envío; y
- III. La certificación de documentos cuando proceda.

Los sujetos obligados deberán esforzarse por reducir al máximo, los costos de entrega de información.

Artículo 69. El sujeto obligado podrá negar el acceso a los datos personales o a realizar la rectificación, cancelación u oposición al tratamiento de éstos, en los siguientes supuestos:

- I. Cuando el solicitante no sea el interesado, o el representante legal no esté debidamente acreditado para ello;
- II. Cuando en el sistema de datos personales de la entidad, no obren los datos

del solicitante;

- III. Cuando se lesionen los derechos de un tercero;
- IV. Cuando exista un impedimento legal, o una resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
- V. Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

La negativa a que se refiere el presente artículo podrá ser parcial, en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el interesado.

Artículo 70. En caso de que no proceda la solicitud, el Área Responsable del Sistema de Datos Personales deberá notificar al interesado, de manera fundada y motivada las razones por las cuales no procedió su solicitud. La respuesta deberá estar firmada por el titular del Área de Responsable del Sistema de Datos Personales.

CAPÍTULO III

DEL RECURSO DE REVISIÓN

Artículo 71. El interesado que se considere agraviado por la resolución que recaiga a su solicitud de acceso, rectificación, cancelación u oposición o ante la omisión de la misma, podrá interponer recurso de revisión ante la Comisión. En este caso, el interesado deberá manifestar su inconformidad por considerar que

la resolución emitida por el sujeto obligado no atendió al contenido de su solicitud.

Para este efecto, el Área de Responsable del Sistema de Datos Personales, al dar respuesta a las solicitudes, orientarán al interesado sobre su derecho de interponer el recurso de revisión y el modo y plazo para hacerlo.

En lo no previsto por esa Ley, durante la sustanciación del recurso de revisión, se aplicará de manera supletoria la Ley del Procedimiento Administrativo del Estado de Tlaxcala y sus Municipios y el Código de Procedimientos Civiles del Estado Libre y Soberano de Tlaxcala.

Artículo 72. El recurso de revisión podrá interponerse ante la Comisión, por escrito o mediante comparecencia.

El recurso se interpondrá por comparecencia, cuando el interesado o su representante legal, acudan ante la Comisión a interponer el recurso, previa acreditación de su personalidad.

El plazo para interponer el recurso de revisión será de quince días hábiles contados a partir de la fecha en que surta efectos la notificación de la resolución administrativa impugnada.

Artículo 73. Cuando la resolución emitida por el sujeto obligado afecte los derechos de acceso, rectificación, cancelación u oposición de datos personales de un menor o incapaz, los padres o tutores de éstos, o su representante legal, según sea el caso, podrán interponer el recurso de revisión, previa acreditación de su personalidad así como del parentesco y entroncamiento con el menor o

incapaz.

Artículo 74. Cuando el recurso de revisión se interponga por escrito, éste deberá contener los requisitos siguientes:

- I. Nombre del interesado o, en su caso, el de su mandatario acompañado del documento que acredite su personalidad;
- II. Nombre del tercero interesado, si lo hubiere;
- III. Domicilio o dirección electrónica para recibir notificaciones, y en su caso el nombre de la o las personas que autorice para tal efecto;
- IV. El nombre y domicilio del sujeto obligado responsable;
- V. El acto o resolución impugnado;
- VI. Los hechos y agravios en que se funde la impugnación, pudiendo anexar las pruebas que sustenten su impugnación, y
- VII. Acompañar original o copia certificada de la resolución definitiva que recaiga a la misma

La Comisión suplirá la deficiencia de la queja a favor del interesado e intervendrá de oficio para garantizar la protección de los datos personales y los principios que lo rigen.

Para efectos de lo dispuesto en el párrafo anterior, cuando el interesado no cumpla con alguno de los requisitos que señala el artículo anterior, la Comisión, en un plazo no mayor a dos días, lo prevendrá para que en un término máximo de tres días contados a partir de aquél en que haya surtido efectos la notificación subsane las irregularidades. Con el apercibimiento de que en caso de no cumplir se tendrá por no interpuesto el recurso.

Artículo 75. Recibido el recurso de revisión, la Comisión lo notificará al sujeto obligado a quien se atribuya el acto o resolución impugnado, a más tardar dentro de los tres días hábiles siguientes, remitiéndole copia simple de las constancias que integran dicho recurso, a efecto de que en un término de cinco días hábiles contados a partir del día siguiente al de su notificación, rinda un informe justificado del acto que se le impugna.

Si dentro del término fijado en el párrafo anterior, no se recibiera el informe justificado, se tendrán por ciertos los hechos señalados por el interesado, siempre que éstos le sean directamente imputables al sujeto obligado, por lo que la Comisión procederá a desahogar las pruebas ofrecidas por el interesado y emitirá la resolución correspondiente.

Artículo 76. Después de recibido el informe justificado por parte del sujeto obligado, el Comisionado Ponente deberá certificar a las partes la fecha de inicio y de conclusión del periodo concedido para ofrecer pruebas y desahogar, el que no podrá exceder de quince días hábiles a partir de que sea legalmente notificado el acuerdo correspondiente.

Las partes podrán ofrecer todo tipo de pruebas, excepto la confesional de los sujetos obligados y aquellas que sean contrarias a derecho. La Comisión señalará las fechas para el desahogo de aquellos medios de prueba que por su propia y especial naturaleza así lo requieran.

En cualquier caso corresponderá a la Comisión, desechar aquellas pruebas que no guarden relación con el recurso.

La Comisión, por conducto del Registro, tendrá acceso a la información contenida en los sistemas de datos personales que resulte indispensable para resolver el recurso. Dicha información deberá ser mantenida con carácter

confidencial y no estará disponible en el expediente.

Artículo 77. Una vez transcurrido el término probatorio concedido a las partes, se fijará fecha para la audiencia de alegatos, los que podrán formularse ante la Comisión, por comparecencia o por escrito.

La audiencia de alegatos a que se refiere el presente artículo deberá celebrarse dentro de los tres días hábiles siguientes a la conclusión del periodo probatorio.

Artículo 78. La resolución que recaiga al recurso de revisión interpuesto, se deberá emitir dentro de los diez días hábiles contados a partir de la fecha en que se haya celebrado la audiencia de alegatos.

Al resolver el recurso de revisión la Comisión podrá:

- I. Desechar el recurso por improcedente o bien, sobreseerlo;
- II. Confirmar el acto o resolución impugnada; y
- III. Revocar o modificar las decisiones del sujeto obligado y solicitarle a éste que permita al interesado el acceso a la información solicitada, que la proporcione completa, que reclasifique la información o bien, que modifique tales datos.

Las resoluciones, siempre deberán constar por escrito, establecerán los plazos para su cumplimiento y los procedimientos para asegurar la ejecución.

Si la Comisión no resuelve recurso de revisión en el plazo establecido en esta Ley, será motivo de responsabilidad.

Artículo 79. En contra de la resolución que resuelva el recurso de revisión interpuesto ante la Comisión, no procederá recurso ordinario alguno.

Artículo 80. Sin perjuicio de lo dispuesto en el presente Capítulo, la Comisión podrá en cualquier momento del procedimiento citar a las partes a una audiencia de conciliación. De resolverse favorablemente el asunto, la Comisión emitirá una resolución en la que haga constar el contenido del acuerdo, el cual tendrá efectos vinculantes para las partes.

CAPÍTULO IV

DE LA IMPROCEDENCIA DEL RECURSO Y DEL SOBRESEIMIENTO

Artículo 81. Será improcedente el recurso de revisión, cuando:

- I. El recurso se interponga fuera de los plazos fijados para tal efecto por esta Ley;
- II. El acto impugnado ya haya sido materia de una resolución anterior emitida por la Comisión;
- III. Se encuentre en trámite ante autoridad jurisdiccional federal competente, algún recurso o medio de defensa intentado por el recurrente;
- IV. Se impugnen actos o resoluciones que no hayan sido emitidos por el sujeto obligado, y
- V. Se interponga contra un acto o resolución con el que haya identidad de partes, pretensiones y actos reclamados, respecto a otro recurso de revisión.

Artículo 82. Procede el sobreseimiento del recurso de revisión:

- I. Si el recurrente se desiste de manera expresa del recurso interpuesto;
- II. Por muerte del recurrente o extinción del sujeto obligado;
- III. Si al admitirse el recurso de revisión, sobrevenga alguna causal de improcedencia de las previstas en la presente Ley, y
- IV. Ante la manifestación expresa de la conformidad con la modificación, cancelación, inclusión, complementación, rectificación, suspensión, reserva o cancelación de los datos personales del recurrente; o bien, ante el desistimiento por escrito de éste respecto de la acción intentada, previa ratificación del mismo, y
- V. Cuando el recurso quede sin materia.

CAPÍTULO V

DE LA EJECUCIÓN DE LAS RESOLUCIONES

Artículo 83. El Comisionado Presidente y la Secretaría Técnica y de Asuntos Jurídicos de la Comisión, serán las áreas encargadas de ejecutar las resoluciones que hubiere pronunciado el Consejo General, con apoyo del Secretario de Estudio que haya conocido del asunto.

Para tal efecto, la Secretaría Técnica y de Asuntos Jurídicos de la Comisión, dictará los acuerdos de ejecución pertinentes, a fin de dar cumplimiento a las determinaciones emitidas por el Consejo General.

Artículo 84. Una vez que haya sido notificada al sujeto obligado, la resolución recaída al recurso de revisión, ésta deberá dar cumplimiento a lo determinado en la misma dentro del término de cinco días hábiles contados a partir del día siguiente al de la notificación respectiva, debiendo informar a la Comisión sobre su cumplimiento.

Ante el incumplimiento a lo dispuesto por el párrafo anterior, la Comisión informará de dicha circunstancia al titular del sujeto obligado o ante su superior jerárquico, según sea procedente, para que instaure el procedimiento sancionador previsto en la Ley de Responsabilidades de los Servidores Públicos para el Estado de Tlaxcala.

Artículo 85. Una vez que haya sido debidamente cumplimentada por el sujeto obligado, la resolución emitida por el Consejo General de la Comisión, se procederá a dictar el acuerdo correspondiente a su conclusión y archivo.

TÍTULO SEXTO

DE LAS INFRACCIONES Y SANCIONES

CAPÍTULO ÚNICO

DE LAS INFRACCIONES

Artículo 86. Constituyen infracciones leves a la presente Ley:

- I. Omitir la inclusión, complementación, rectificación, actualización, reserva, suspensión o cancelación, de oficio o a petición del interesado, de los

- datos personales que obren en sistemas de datos personales;
- II. Incumplir las instrucciones dictadas por el responsable del archivo, registro, base o banco de datos del sujeto obligado del que dependa;
 - III. Crear los sujetos obligados el sistema de datos de carácter personal, sin haber sido notificado previamente a la Comisión ni haberse hecho la publicación respectiva de la resolución de la creación de dicho sistema en el Periódico Oficial del Gobierno del Estado de Tlaxcala;
 - IV. Omitir la publicación respectiva de la resolución de la modificación o supresión del sistema de datos personales en el Periódico Oficial del Gobierno del Estado de Tlaxcala, así como la respectiva notificación a la Comisión;
 - V. Recabar datos de carácter personal sin proporcionar la información prevista en la presente Ley;
 - VI. Omitir sin razón fundada, la atención de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;
 - VII. Crear un sistema de datos personales sin proporcionar la información prevista en esta ley así como omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el párrafo tercero del artículo 14;
 - VIII. Actuar con negligencia, dolo o mala fe en la tramitación sustentación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales, dentro de los plazos previstos así como el no comunicar al solicitante cuando la solicitud no sea de su competencia, y
 - IX. Cualquiera otra de carácter puramente formal o documental que no pueda ser catalogada como grave;

Artículo 87. Son infracciones graves en materia de datos personales:

- I. Obtener o tratar datos personales para constituir o implementar registros de datos de titularidad pública, sin que esté prevista su autorización por la norma aplicable;
- II. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en la base de datos del responsable del sujeto obligado;
- III. Obtener o tratar automatizadamente datos personales para constituir o implementar un registro de datos de titularidad privada, sin el consentimiento del interesado o de quien legítimamente puede otorgarlo;
- IV. Obtener o tratar automatizadamente o administrar datos de carácter personal con violación a los principios que rigen esta Ley o de las disposiciones que sobre protección y seguridad de datos sean vigentes;
- V. Impedir u obstaculizar de manera injustificada, el ejercicio de los derechos de acceso;
- VI. Violentar el secreto profesional que debe guardar por disposición de esta Ley;
- VII. Omitir total o parcialmente el cumplimiento de las resoluciones emitidas por la Comisión, así como obstruir las funciones de la misma;
- VIII. Omitir o presentar de manera extemporánea los informes a que se refiere la presente Ley;
- IX. Obtener datos personales de manera engañosa o fraudulenta;
- X. Transferir datos personales, fuera de los supuestos permitidos, particularmente cuando la transmisión haya tenido por objeto obtener un lucro indebido;
- XI. Impedir u obstaculizar la inspección ordenada por la Comisión;
- XII. Destruir, alterar, ceder datos personales, archivos o sistemas de datos personales sin autorización del interesado;
- XIII. Incumplir con la inmovilización de sistemas de datos personales

ordenada por la Comisión, y

- XIV. Mantener archivos, registros, bases o bancos de datos, inmuebles, equipos o herramientas sin las condiciones mínimas de seguridad requeridas por esta Ley y demás disposiciones legales aplicables.

Artículo 88. La Comisión denunciará ante las autoridades competentes cualquier conducta prevista en el artículo anterior y aportará las pruebas que considere pertinentes para efectos de que, en tratándose de infracciones cometidas por servidores públicos, se proceda a sancionar administrativamente a dicho servidor conforme a lo dispuesto por los artículos 66 al 75 de la Ley de Responsabilidades de los Servidores Públicos para el Estado de Tlaxcala, con independencia de las responsabilidades civiles o penales que procedan.

Los órganos de control y fiscalización internos de las entidades públicas deberán entregar semestralmente a la Comisión, un informe estadístico de los procedimientos administrativos iniciados con motivo del incumplimiento de la presente Ley y sus resultados. Esta información será incorporada al informe anual de la Comisión.

Artículo 89. Además de las denuncias sobre las faltas administrativas cometidas por servidores públicos con motivo del incumplimiento de la presente Ley, la Comisión podrá solicitar al titular de la dependencia o ante su superior jerárquico, la amonestación pública o privada, según el caso.

La Comisión dará seguimiento a las actuaciones y diligencias que se practiquen con motivo del procedimiento administrativo que el sujeto obligado integre o instruya en contra de él o los servidores públicos infractores. Esta facultad se

limitará únicamente a la observación atenta del curso del asunto de que se trate hasta su resolución definitiva, sin que en ningún caso se entienda como la posibilidad de intervenir como parte en aquéllos, haciendo o promoviendo las diligencias conducentes para su resolución.

Artículo 90. Una vez emitida la resolución derivada del procedimiento sancionador instaurado en contra de él o los servidores públicos infractores a las disposiciones de la presente Ley, dentro de los tres días hábiles posteriores, deberá comunicar el sentido de dicha resolución a la Comisión.

La Comisión, de manera inmediata, notificará al interesado el sentido de la resolución emitida por el sujeto obligado, para que si éste considera que la resolución emitida es contraria a derecho o no se encuentra debidamente fundada y motivada, pueda inconformarse con el sentido de dicha resolución, a través del recurso de revocación, ante la autoridad que la haya emitido, conforme a las reglas del Código de Procedimientos Penales.

TRANSITORIOS

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

ARTÍCULO SEGUNDO. La Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala, expedirá el Reglamento de esta Ley dentro de los sesenta días posteriores a la entrada en vigor de la presente Ley.

ARTÍCULO TERCERO. Una vez entrada en vigor la presente Ley, la Comisión realizará las previsiones presupuestales necesarias para dotar de los recursos económicos, materiales y humanos necesarios para el funcionamiento del Registro Estatal de Protección de Datos Personales.

ARTÍCULO CUARTO. Los sujetos obligados que administren o pretendan administrar sistemas de datos personales, deberán notificar a La Comisión, dentro de los treinta días hábiles posteriores a la entrada en vigor de la presente Ley, la relación de los sistemas que posean para que se proceda a su inscripción en el Registro.

ARTÍCULO QUINTO. Los titulares u órganos de gobierno de los sujetos obligados, designarán a la persona responsable del sistema de datos personales a que se refiere el artículo 40 de la presente Ley, dentro de los sesenta días posteriores a la entrada en vigor de este ordenamiento legal.

ARTÍCULO SEXTO. Los interesados podrán ejercer ante los responsables sus derechos de acceso, rectificación, cancelación y oposición contemplados en el Título Quinto de la Ley, dentro de los noventa días posteriores a la entrada en vigor de la Ley.

ARTÍCULO SÉPTIMO. Se derogan todas aquellas disposiciones que se contrapongan a la presente Ley.

AL EJECUTIVO, PARA QUE LO SANCIONE Y MANDE PUBLICAR

