PUBLICADO EN LA GACETA OFICIAL DEL ESTADO
NÚM. EXT. 338 DE FECHA 2 DE OCTUBRE DE 2012.

GOBIERNO DEL ESTADO

PODER EJECUTIVO

Al margen un sello que dice: Estados Unidos Mexicanos.— Gobernador del Estado de Veracruz de Ignacio de la Llave.

Xalapa-Enríquez, septiembre 26 de 2012.
Oficio número: 279/2012.
Septiembre, Mes de la Protección Civil.

Javier Duarte de Ochoa, Gobernador del Estado Libre y Soberano de Veracruz de Ignacio de la Llave, a sus habitantes sabed:

Que la Sexagésima Segunda Legislatura del Honorable Congreso del Estado se ha servido dirigirme la siguiente Ley para su promulgación y publicación:

Al margen un sello que dice: Estados Unidos Mexicanos.— Poder Legislativo.— Estado Libre y Soberano de Veracruz de Ignacio de la Llave.

La Sexagésima Segunda Legislatura del Honorable Congreso del Estado Libre y Soberano de Veracruz de Ignacio de la Llave, en uso de la facultad que le confieren los artículos 33 fracción I y 38 de la Constitución Política local, 18 fracción I y 47 segundo párrafo de la Ley Orgánica del Poder Legislativo; 75 y 76 del Reglamento para el Gobierno Interior del Poder Legislativo; y en nombre del pueblo expide la siguiente:

LEY NÚMERO 581

PARA LA TUTELA DE LOS DATOS PERSONALES EN EL ESTADO DE VERACRUZ DE IGNACIO DE LA LLAVE

TÍTULO PRIMERO

CAPÍTULO ÚNICO
Disposiciones Generales

Artículo 1. La presente Ley es de orden público e interés general y tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos.

Artículo 2. El derecho humano a la protección de los datos personales deberá interpretarse de conformidad con la Constitución Política de los Estados Unidos Mexicanos, la del Estado de Veracruz de Ignacio de la Llave, 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.

Artículo 3. Los entes públicos, en el ámbito de su competencia, deberán promover, respetar, proteger y garantizar la seguridad de los datos personales que obren en su poder, de conformidad con los principios establecidos en la presente Ley.

Artículo 4. Los datos personales son irrenunciables, intransferibles e indelegables, salvo disposición legal o cuando medie el consentimiento de su titular.

Artículo 5. En todo lo no previsto por el presente ordenamiento se aplicarán supletoriamente la Ley de Transparencia y Acceso a la Información Pública y el Código de Procedimientos Administrativos para el Estado.

Artículo 6. Para los efectos de la presente Ley, se entiende por:

I. **Bloqueo de datos personales:** La identificación y reserva con carácter temporal de datos personales, con el fin de impedir su tratamiento;

II. **Cancelación:** Eliminación de determinados datos de un sistema de datos personales, previo bloqueo de los mismos;

III. **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 entes públicos;

IV. **Datos personales:** La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable, concerniente a su origen étnico, características físicas, morales o emocionales, vida afectiva y familiar, domicilio y teléfono particulares, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, huella digital, ADN y número de seguridad social, u otros similares.

V. **Declarativa de privacidad:** Documento emitido por el responsable del sistema de datos personales al titular de éstos, como garantía de reserva en el tratamiento de los mismos;

VI. **Ente Público:** El Poder Ejecutivo, sus dependencias centralizadas y entidades paraestatales; el Poder Legislativo, sus comisiones y órganos administrativos, y aquellos que de manera individual o por grupos legislativos establezcan los diputados locales; el Poder Judicial, sus órganos jurisdiccionales y administrativos; los Ayuntamientos o Concejos Municipales, las dependencias de la administración pública municipal y entidades paramunicipales; las entidades paramunicipales creadas por dos o más ayuntamientos; los Organismos Autónomos del Estado y los que adquieran tal carácter por mandato de ley; los Partidos y Asociaciones Políticas con registro en el Estado, y los que reciban prerrogativas en la entidad; los notarios públicos; las organizaciones de la sociedad civil constituidas conforme a las leyes mexicanas que reciban recursos públicos; los particulares que desempeñen servicios y funciones públicas, por encargo, comisión, concesión o cualquier otro acto jurídico que implique la delegación o ejercicio del servicio o función; así como las personas de derecho público o privado que, en razón de un acto o hecho jurídico, se relacionen con un ente público y, como consecuencia de ello, se creen bases de datos personales o se realice el tratamiento de éstos;

VII. **Estado:** El Estado de Veracruz de Ignacio de la Llave;

VIII. **Ficheros de control de acceso:** Registros de datos personales que se requieren para controlar las entradas y salidas a un edificio público;

IX. **Instituto:** El Instituto Veracruzano de Acceso a la Información;

X. **Procedimiento de disociación:** Todo tratamiento de datos personales que permita que la información que se obtenga no pueda asociarse a una persona física identificada o identificable;

XI. **Responsable del Sistema de Datos Personales:** Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos;

XII. **Sistema de Datos Personales:** Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;

XIII. **Titular:** Persona física a quien se refieren los datos personales que sean objeto del tratamiento previsto en la presente Ley;

XIV. **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados, informáticos, manuales, mecánicos, digitales o electrónicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, cotejo o 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, así como su bloqueo, supresión o destrucción;

XV. **Unidad de Acceso a la Información Pública:** La unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los entes públicos, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida el Instituto; y

XVI. **Usuario:** Aquel autorizado por el ente público para prestarle servicios para el tratamiento de datos personales.

Artículo 7. El tratamiento, manejo, aplicación, custodia, almacenamiento o cualquier otro acto que tenga por objeto los datos personales estará sujeto al cumplimiento de los siguientes principios y garantías:

I. **Calidad de los datos:** Los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados. La información deberá recopilarse para un propósito legal directamente relacionado con una función o actividad del servicio público. El responsable de la información deberá tomar las medidas necesarias para garantizar que, teniendo en cuenta la finalidad para la que se recopila la información, ésta es relevante para ese fin y está al día y completa, y que el acopio de la información no incida, interfiera o se entrometa, en una medida razonable, en los asuntos personales del interesado;

II. **Legitimación del tratamiento:** El tratamiento de datos personales sólo podrá efectuarse si el titular ha dado su consentimiento de forma expresa o si el tratamiento es necesario para la ejecución de un contrato en el que el titular sea parte, o el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o proteger el interés vital del titular, o el cumplimiento de una misión de interés público, o la satisfacción del interés legítimo perseguido por el responsable del tratamiento. En caso de que el responsable de la información la requiera para un fin distinto, el titular deberá dar su consentimiento al uso de la información para ese otro propósito;

III. **Categorías especiales de tratamiento:** Se prohíbe el tratamiento de datos personales relativos al origen étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, la salud o la sexualidad, así como cualquier otro dato análogo cuya divulgación pueda afectar la intimidad de las personas. Esta disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico;

IV. **Información a los afectados por el tratamiento:** El responsable del tratamiento informará al interesado el propósito para el cual se solicita la información; si la recolección de la información se autoriza o requiera por algún dispositivo legal o en virtud de la prestación de un servicio o función de derecho público, así como la identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, y cualquier otra información que se considere necesaria para lograr el consentimiento informado del uso de los datos personales por parte del interesado;

V. **Derecho de acceso del interesado a los datos:** Los interesados tendrán el derecho de obtener del responsable del tratamiento la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos; la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Ley, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones;

VI. **Excepciones y limitaciones:** Podrá limitarse el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante o la protección del interesado;

VII. **Derecho del interesado a oponerse al tratamiento:** El interesado podrá oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento o se comuniquen a terceros para efectos de prospección, por lo que cuando ello se pretenda deberá informársele oportunamente;

VIII. **Confidencialidad y seguridad del tratamiento:** Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Al efecto, éste deberá aplicar las medidas adecuadas para que el registro esté protegido por las garantías de seguridad, frente a la pérdida, acceso no autorizado, uso, modificación o divulgación, y en contra de cualquier otra utilización indebida;

IX. **Notificación del tratamiento a la autoridad de control:** El responsable del tratamiento efectuará una notificación al Instituto con anterioridad a la realización de un tratamiento. El Instituto realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados; y

X. **Proporcionalidad:** Sólo podrán obtenerse y ser sujeto de tratamiento los datos personales cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades expresas y legítimas para los que se hayan obtenido.

Artículo 8. La disposición contenida en la fracción III del artículo anterior, referente a la prohibición del tratamiento de datos personales, no se aplicará cuando éste sea:

I. Consentido expresamente por el titular;

II. Necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia laboral, en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas;

III. Ineludible para salvaguardar el interés vital del titular o de otra persona, en el supuesto de que el titular esté física o jurídicamente incapacitado para dar su consentimiento;

IV. Efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y que los datos no se comuniquen a terceros sin el consentimiento de los titulares;

V. Referente a datos que el titular haya hecho manifiestamente públicos, o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; y

VI. Necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto legalmente al secreto profesional, o por otra persona obligada igualmente al secreto.

Artículo 9. Los instrumentos jurídicos que correspondan a la contratación de servicios del responsable del sistema de datos personales, en cualquier modalidad, así como de los usuarios, deberán prever la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación y las penas convencionales por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades 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 medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.

TÍTULO SEGUNDO
Sistemas de Datos Personales

CAPÍTULO I
Disposiciones Generales

Artículo 10. Cada ente público determinará, a través de su titular o, en su caso, del área correspondiente, la creación, modificación o supresión de sistemas de datos personales, conforme a su ámbito de competencia, con respeto a los principios y garantías establecidos en esta Ley.

La creación, modificación o supresión de sistemas se realizará mediante acuerdo que deberá publicarse en la Gaceta Oficial del estado y en la página institucional de internet del ente público, y que deberá contener:

I. La finalidad del sistema de datos personales y los usos previstos para el mismo;

II. El origen de los datos y el grupo de interesados al que va dirigido;

III. Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;

IV. El procedimiento de recopilación de los datos de carácter personal;

V. La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo;

VI. La cesión de la que puedan ser objeto los datos;

VII. Las instancias responsables del tratamiento del sistema de datos personales;

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

IX. El plazo de conservación de los datos; y

X. El nivel de protección exigible.

Artículo 11. Los sistemas de datos personales deberán suprimirse una vez concluidos los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines por los cuales fueron recabados.

El acuerdo de supresión deberá contener:

I. El destino que vaya a darse a los datos contenidos en el sistema, o en su caso, las previsiones que se adopten para su destrucción;

II. La conservación de datos con finalidades estadísticas o históricas, previamente sometidos al procedimiento de disociación; y

III. La notificación al Instituto y publicación del acuerdo en la *Gaceta Oficial* del estado.

Artículo 12. Todos los acuerdos a que se refiere el presente Capítulo deberán contener una exposición considerativa donde se expresen la fundamentación y motivación correspondientes.

Artículo 13. Los sistemas de datos personales en posesión de los entes públicos deberán inscribirse en el registro que al efecto habilite el Instituto.

El registro deberá comprender como mínimo la información siguiente:

I. Naturaleza de la información y su registro;

II. Objetivos para los cuales se utiliza la información;

III. Medidas que deben tomarse si se desea tener acceso al expediente;

IV. Finalidad y periodo para el que se mantiene cada tipo de registro;

V. Personas que tienen derecho de acceso a la información personal contenida en los registros y las condiciones para este derecho;

VI. Nombre, correo electrónico, dirección, teléfono y cargo del responsable, así como nombre de los usuarios; VII. Forma de recopilación y actualización de datos;

VII. Destino de los datos y personas físicas o morales a las que pueden ser transmitidos;

VIII. Modo de interrelacionar la información registrada;

IX. Fecha de publicación en la *Gaceta Oficial* del estado;

X. Normatividad aplicable al sistema, y

XI. Medidas de seguridad.

Artículo 14. Cuando los entes públicos recaben datos personales deberán informar previamente a los titulares de forma expresa, precisa e inequívoca, mediante la declarativa de privacidad correspondiente:

I. De la existencia de un sistema de datos personales, del tratamiento de datos personales, de la finalidad de la obtención de éstos y de los destinatarios de la información;

II. Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas;

III. De las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos;

IV. De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del titular, salvo cuando se trate de datos personales que por disposición de una Ley sean considerados públicos;

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

VI. Del nombre, domicilio, teléfono, correo electrónico y cargo del responsable del sistema de datos personales y en su caso de los destinatarios; y

VII. Del nivel de las medidas de seguridad adoptadas.

Cuando se utilicen cuestionarios u otros impresos para la obtención de los datos, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el presente artículo.

Artículo 15. En caso de que los datos de carácter personal no hayan sido obtenidos del titular, 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 la información tenga el carácter de pública o sea necesaria para el cumplimiento de algún deber legal, o cuando los datos personales procedan de fuentes accesibles al público en general.

Artículo 16. Los datos personales que divulguen los entes públicos serán exactos y actualizados, por lo que éstos deberán sustituir, rectificar o completar oficiosamente los que publiquen y resulten inexactos o incompletos.

Artículo 17. Ninguna persona está obligada a proporcionar datos personales cuya utilización indebida pueda dar origen o conlleve un riesgo grave para el titular, quedando prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenarlos y sólo podrán ser tratados cuando medien razones de interés general, así lo disponga una ley, lo consienta expresamente el

titular o, con fines estadísticos o históricos, siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

CAPÍTULO II
Registros Públicos

Artículo 18. El tratamiento de los sistemas de datos personales en materia de registros públicos, como el Registro Público de la Propiedad y el Registro Civil, se rige por lo dispuesto en sus leyes especiales. A pesar de lo anterior, los entes públicos respectivos deberán ajustar su normatividad y su gestión a los principios, garantías y deberes contenidos en esta Ley, en lo relativo a los servicios de consulta de sus bases de datos, la reproducción y transmisión por cualquier medio de la información que posean, así como por cuanto a las medidas de seguridad que deben adoptar.

CAPÍTULO III
Historial Clínico

Artículo 19. El tratamiento de los sistemas de datos personales en materia de salud se rige por lo dispuesto en la Ley General de Salud, la Ley de Salud para el Estado y demás normas que de ellas deriven.

A pesar de lo anterior, los entes públicos respectivos deberán ajustar su normatividad y su gestión, a los principios, garantías y deberes contenidos en esta Ley, en especial lo relativo a la consulta de sus bases de datos, la reproducción y transmisión por cualquier medio de la información que posean, así como por cuanto a las medidas de seguridad que deben adoptar.

En lo que no se contravengan disposiciones especiales en materia de salud, el acceso al historial o expediente clínico con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

CAPÍTULO IV
Seguridad Pública

Artículo 20. 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.

Artículo 21. 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.

Artículo 22. La obtención y tratamiento de los datos a los que se refiere el presente Capítulo podrán realizarse sólo 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 titulares ante los órganos jurisdiccionales.

A estos efectos, se considerará especialmente la edad del titular 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 23. Los datos personales recabados con fines policiales se cancelarán cuando no sean necesarios para las investigaciones que motivaron su almacenamiento, con excepción de los que obren en poder de autoridades, mismas que privilegiarán la seguridad de las personas y de la sociedad en general, respecto del crimen tanto común como organizado, por lo que deberán establecer bases de datos de consulta pública referentes a criminales convictos, sobre la base de que la privacidad de esos datos es menos importante que el interés del gobierno por mantener la seguridad pública. Para lograr lo anterior deberán coordinarse con el Instituto, a fin de emitir los lineamientos y disposiciones necesarios.

Artículo 24. El registro y tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad sólo podrá efectuarse bajo el control de la autoridad competente y con estricto apego a las disposiciones aplicables.

Artículo 25. 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 en el cumplimiento de sus atribuciones.

CAPÍTULO V
Video-Vigilancia y Ficheros de Control de Acceso

Artículo 26. Cuando la utilización de sistemas de vigilancia mediante videocámaras dé lugar a la creación de ficheros donde se almacenen las imágenes en un disco duro, o en cualquier otro soporte informático, que permitan localizarlas atendiendo a criterios como el día y hora de grabación, el cruce de imágenes o el lugar físico registrado, el ente público deberá colocar de manera visible y de fácil localización la señalización correspondiente, en la que se indique la zona que es objeto de video vigilancia.

Cuando las imágenes almacenadas se asocien a un fichero de control de acceso, en la declarativa de privacidad se establecerá como mínimo:

I. La existencia de un fichero o tratamiento de datos de carácter personal, la finalidad de la recopilación de éstos y los destinatarios de la información;

II. El carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas;

III. Las consecuencias de la obtención de los datos o de la negativa a suministrarlos;

IV. La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y

V. La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

CAPÍTULO VI
Boletines Judiciales, Listas de Acuerdos y Estrados

Artículo 27. Las notificaciones por lista de acuerdos, estrados y boletines judiciales se ajustarán a lo dispuesto por las leyes especiales, pero deberán adoptar los principios y garantías contenidos en esta Ley en la protección de los datos personales.

Artículo 28. Si la publicación de los datos personales lleva por fin la notificación al titular de un determinado acto, y la notificación se realiza por medios informáticos, digitales o de internet, una vez efectuada aquélla y transcurridos los plazos de ejercicio de los posibles recursos, no se mantendrán dichos datos para su localización a través de los buscadores electrónicos. Al efecto, se dictarán las órdenes oportunas para limitar la indexación del nombre y apellidos de las personas en los mencionados documentos mediante la incorporación de un código norobot.txt, con objeto de que los motores de búsqueda de internet no puedan asociarlo al titular.

CAPÍTULO VII
Medidas de Seguridad

Artículo 29. Los entes públicos establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integridad de cada sistema de datos personales que posean, con la finalidad de proteger los datos de carácter personal tratados de posibles incidencias que puedan provocar su pérdida, alteración o acceso no autorizado, tanto interno como externo, preservando el pleno ejercicio de los derechos tutelados en la presente Ley.

Las medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, deberán constar por escrito y ser comunicadas al Instituto para su registro. Asimismo, deberán indicar el nombre y cargo del servidor público o, en su caso, la persona física o moral que intervenga en el tratamiento de datos personales con el carácter de responsable del sistema o usuario, según corresponda. Cuando se trate de usuarios, deberán incluirse los datos del acto jurídico mediante el cual el ente público otorgó el tratamiento del sistema de datos personales.

En el supuesto de actualización de estos datos, la modificación respectiva deberá notificarse al Instituto dentro de los treinta días hábiles siguientes a la fecha en que se efectuó.

Artículo 30. El ente público responsable de la tutela y tratamiento del sistema de datos personales adoptará las medidas de seguridad conforme a lo siguiente:

I. Tipos de seguridad:

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

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

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

d) **De cifrado.** Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información; y

e) **De comunicaciones y redes.** Se refiere a las restricciones preventivas o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

II. Niveles de seguridad:

a) **Básico.** El relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos:

1. Documento de seguridad;

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

3. Registro de incidencias;

4. Identificación y autentificación;

5. Control de acceso;

6. Gestión de soportes; y

7. Copias de respaldo y recuperación.

b) **Medio.** Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos personales suficientes para obtener una evaluación de la personalidad del individuo.

Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos:

1. Responsable de seguridad;

2. Auditoría;

3. Control de acceso físico; y

4. Pruebas con datos reales.

c) **Alto.** Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen 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:

1. Distribución de soportes;

2. Registro de acceso; y

3. Telecomunicaciones.

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

Artículo 31. Las medidas de seguridad de los datos personales tratados en bases de datos almacenadas o soportadas en sistemas informáticos deberán ser analizadas y establecidas por medio del Comité de Información de Acceso Restringido a que se refiere el artículo 13 de la Ley de Transparencia y Acceso a la Información Pública para el Estado, que se constituirá como el Comité para la Seguridad Informática de los Datos Personales.

Artículo 32. El responsable del área informática de cada ente público deberá integrarse de manera obligatoria al Comité de Información de Acceso Restringido, el que deberá:

I. Elaborar el análisis de riesgos de las tecnologías de la información del ente público;

II. Desarrollar metodologías y procesos específicos relativos a la seguridad y privacidad de la información;

III. Desarrollar el proceso de administración de la continuidad de las operaciones de las tecnologías de la información y las comunicaciones de tratamiento de información del ente público ante la presencia de incidentes relativos a la seguridad de la información;

IV. Proponer al Comité de Seguridad del ente público, para su aprobación, la política de seguridad de la información y sus objetivos, de conformidad con los lineamientos que al efecto emita el Instituto, así como observar el cumplimiento de los mismos;

V. Establecer, operar, monitorear, mantener y mejorar un sistema de administración de seguridad de la información;

VI. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;

VII. Garantizar que la seguridad sea parte del proceso de planificación de la información;

VIII. Conformar grupos de trabajo que permitan garantizar la seguridad y privacidad de los entes públicos; y

IX. Promover la difusión de la cultura de seguridad y privacidad de la información dentro del ente público.

Artículo 33. Las medidas de seguridad a las que se refiere el presente Capítulo constituyen mínimos exigibles, por lo que el ente público adoptará las medidas adicionales que estime 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 al Instituto, para su registro, el nivel de seguridad aplicable.

Los entes públicos podrán hacer referencia a estándares, normas, marcos de referencia y buenas prácticas estatales, nacionales e internacionales, a fin de establecer las medidas de seguridad que ofrezcan mayor garantía para la protección de los datos personales.

CAPÍTULO VIII
Tratamiento de Datos Personales

Artículo 34. El tratamiento de los datos personales requerirá el consentimiento inequívoco, expreso y por escrito del titular, excepto cuando:

I. Se recaben para el ejercicio de las atribuciones legales conferidas a los entes públicos;

II. Exista una orden judicial;

III. 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. El titular no esté en posibilidad de otorgar su consentimiento por motivos de salud y el tratamiento de sus datos resulte necesario para la prevención o 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. La transmisión se encuentre expresamente prevista en una ley;

VI. La transmisión se produzca entre entes públicos, u organismos públicos del fuero federal o del ámbito internacional, y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos;

VII. 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. 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. Los datos figuren en registros públicos en general y su tratamiento sea necesario siempre que no se vulneren los derechos y libertades fundamentales del titular.

Artículo 35. El consentimiento para recabar y tratar los datos no implica consentir en la cesión de tales datos a terceros; constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de tales datos. Por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recopilación, aun cuando puedan ser compatibles con éstos, implica una nueva posesión y uso que requiere el consentimiento del titular.

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.

El ente público 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, de las personas a que haga referencia la información. Al efecto, la Unidad de Acceso a la Información Pública 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 36. En los supuestos de utilización o cesión de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de derechos de las personas, el Instituto 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, el Instituto podrá bloquear tales sistemas, de conformidad con el procedimiento que al efecto se establezca. El incumplimiento a la inmovilización ordenada por el Instituto será sancionado por éste atendiendo a lo establecido en el Título de Responsabilidades y Sanciones de esta Ley, con independencia de las quejas que los ciudadanos puedan interponer ante los órganos de control interno de los entes públicos.

Artículo 37. 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 ente público, el instrumento jurídico que dio origen al mismo establecerá el plazo de conservación por el usuario, al término del cual los datos serán devueltos en su totalidad al ente público, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

Artículo 38. En caso de que los destinatarios de los datos sean instituciones de la Federación u otras entidades federativas, los entes públicos 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 ente público de que se trate.

En el supuesto de que 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.

CAPÍTULO IX
Del Responsable de los Sistemas de Datos Personales

Artículo 39. El responsable de los sistemas de datos personales es el titular de la Unidad de Acceso a la Información Pública de cada ente público, quien deberá:

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

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

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

IV. Informar al titular, al momento de recabar sus datos, sobre la existencia y finalidad de los sistemas de datos personales, así como el carácter obligatorio u optativo de proporcionarlos y las consecuencias de ello;

V. 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;

VI. Vigilar que en el ente público se utilicen los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;

VII. Permitir en todo momento al titular 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;

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

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

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

XI. Determinar sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales;

XII. 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;

XIII. Coordinarse con el encargado del área de sistemas informáticos del ente público, para la adopción de las medidas de seguridad a que se encuentren sometidos los sistemas de datos personales, que se almacenen en discos duros o cualquier otro mecanismo que proporcionen las tecnologías de la información y comunicaciones, de acuerdo con la normativa vigente; en caso de que el registro sea manual o mecanizado la coordinación deberá realizarse con los titulares de las áreas respectivas del ente público;

XIV. 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 u oposición de datos personales; y

XV. Las demás que se deriven de la presente Ley o demás ordenamientos jurídicos aplicables.

Artículo 40. El titular del ente público será el responsable de decidir sobre la finalidad, contenido y uso del tratamiento del sistema de datos personales, quien podrá delegar dicha atribución en la unidad administrativa en la que se concrete la competencia material, a cuyo ejercicio sirva instrumentalmente el sistema de datos y esté adscrito el responsable del mismo.

TÍTULO TERCERO

CAPÍTULO ÚNICO
Autoridad Responsable del Control y Vigilancia

Artículo 41. El Instituto 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 y tendrá las atribuciones siguientes:

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

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

III. Establecer sistemas electrónicos para la recepción y trámite de solicitudes de acceso, rectificación, cancelación y oposición de datos personales, o utilizar el sistema INFOMEX-Veracruz;

IV. Establecer el registro de los sistemas de datos personales en posesión de los entes públicos;

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

VI. Emitir opiniones sobre temas relacionados con la presente Ley, así como formular observaciones y recomendaciones a los entes públicos, derivadas del incumplimiento de los principios que rigen este ordenamiento;

VII. Hacer del conocimiento del órgano de control interno del ente público que corresponda las resoluciones que emita relacionadas con la probable violación a las disposiciones materia de la presente Ley;

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

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

X. Solicitar y evaluar los informes presentados por los entes públicos respecto del ejercicio de los derechos previstos en esta Ley; en dicha evaluación se incluirá:

a) El número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante cada ente público, así como su resultado;

b) El tiempo de respuesta a la solicitud;

c) El estado que guardan las denuncias presentadas ante los órganos internos de control y las dificultades observadas en el cumplimiento de esta Ley;

d) El uso de los recursos públicos en la materia;

e) Las acciones desarrolladas;

f) Sus indicadores de gestión; y

g) El impacto de su actuación.

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

XII. Establecer programas de capacitación en materia de protección de datos personales y promover acciones que faciliten a los entes públicos 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 de los temas que ponderen la importancia del derecho a la protección de datos personales;

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

XV. Substanciar y resolver el recurso de revisión en los términos previstos en esta Ley y en la Ley de Transparencia y Acceso a la Información Pública para el Estado;

XVI. Evaluar la actuación de los entes públicos, 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;

XVII. Procurar la conciliación de los intereses de los titulares con los de los entes públicos, cuando éstos entren en conflicto con motivo de la aplicación de la presente Ley; y

XVIII. Las demás que establezcan esta Ley y demás ordenamientos aplicables.

Artículo 42. El Instituto contará con un Director de Datos Personales, que durará en su cargo tres años, podrá ser ratificado por otro período igual y será designado por mayoría de los Consejeros. El Director de Datos Personales asistirá al Consejo General del Instituto en el ejercicio de las atribuciones a que se refiere el artículo anterior y lo auxiliará en la resolución de los recursos de revisión de esta naturaleza, conforme a los acuerdos y órdenes que dicte el Consejo, contando para ello con el personal necesario de acuerdo a la disponibilidad presupuestal.

Artículo 43. El Director de Datos Personales deberá ser ciudadano veracruzano, mayor de treinta y cinco años, gozar de buena reputación, prestigio profesional y, al día de su nombramiento, contar con título profesional expedido por autoridad o institución legalmente facultada para ello, con una antigüedad mínima de cinco años. Además, no haber sido condenado por delito doloso ni ser ministro de culto religioso.

El Director de Datos Personales tendrá las atribuciones siguientes:

I. Asistir al Consejo General del Instituto en el ejercicio de las atribuciones conferidas por la presente Ley;

II. Asistir a los Consejeros en la sustanciación y resolución de los recursos de revisión promovidos para garantizar la protección y el debido tratamiento de datos personales, incluida la revisión de los proyectos de resolución;

III. Proveer lo necesario para el cumplimiento de las resoluciones del Consejo General en los recursos de revisión de esta naturaleza; y

IV. Las demás que expresamente le confieran esta Ley, las leyes del Estado y demás disposiciones aplicables.

TÍTULO CUARTO
Del Derecho de Acceso, Rectificación, Cancelación y Oposición y del Procedimiento para su Ejercicio

CAPÍTULO I
Derechos de Acceso, Rectificación, Cancelación y Oposición

Artículo 44. Todo titular, previa identificación mediante documento oficial, contará con los derechos de acceso, rectificación, cancelación y oposición de sus datos personales en posesión de los entes públicos, 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.

La respuesta al ejercicio de cualquiera de los derechos previstos en la presente Ley deberá ser proporcionada en forma inteligible, pudiendo suministrarse, a opción del titular, por escrito o mediante consulta directa.

Artículo 45. El derecho de acceso se ejercerá para solicitar y obtener información de los datos personales sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevea realizar respecto de éstos, en términos de lo dispuesto por esta Ley.

Artículo 46. Procederá el derecho de rectificación de datos del titular, en los sistemas de datos personales, cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos, siempre y cuando la rectificación no esté expresamente prohibida, signifique alterar la verdad jurídica, resulte materialmente imposible o exija esfuerzos desproporcionados.

Artículo 47. El titular 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 el Instituto, 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 entes públicos, para la atención de las posibles responsabilidades nacidas del tratamiento, 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.

Artículo 48. El titular tendrá derecho a oponerse al tratamiento de los datos que le conciernan, en el supuesto en que los datos se hubiesen recabado 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 titular.

Artículo 49. Si los datos rectificados 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, quien deberá también proceder a la rectificación o cancelación de los mismos.

CAPÍTULO II
Procedimiento para el Ejercicio

Artículo 50. La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos per sonales que se formulen a los entes públicos se sujetarán al procedimiento establecido en el presente Capítulo.

Artículo 51. Sin perjuicio de lo que dispongan otras leyes, sólo el titular o su representante legal, previa acreditación de su personalidad, podrá solicitar al ente público, a través de la Unidad de Acceso a la Información Pública, 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 en posesión del ente público.

Artículo 52. La Unidad de Acceso a la Información Pública del ente público deberá notificar al solicitante 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 ésta, 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 párrafo anterior, podrá ser ampliado una sola vez, por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Si la información proporcionada por el solicitante es insuficiente para localizar los datos personales o éstos son erróneos, la Unidad de Acceso a la Información Pública del ente público 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 ésta, apercibido 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 ente público y éste considere improcedente la solicitud de acceso, rectificación, cancelación u oposición, deberá emitirse una resolución fundada y motivada al respecto. Dicha respuesta deberá estar firmada por el titular de la Unidad de Acceso a la Información Pública y por el responsable del sistema de datos personales del ente público.

Artículo 53. 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 ente público, se hará del conocimiento del titular 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 el titular del órgano de control interno y el titular de la Unidad de Acceso a la Información Pública, en su carácter de responsable del sistema de datos personales del ente público.

Artículo 54. La solicitud de acceso, rectificación, cancelación u oposición de datos personales, se podrá presentar en cualquiera de las siguientes modalidades:

I. Por escrito material, que se presentará personalmente por el titular o su representante legal, en la Unidad de Acceso a la Información Pública, o bien a través de correo ordinario, correo certificado o servicio de mensajería;

II. Por correo electrónico, que realizará el titular a través de una dirección electrónica y se enviará a la dirección de correo electrónico asignada a la Unidad de Acceso a la Información Pública del ente público; y

III. Por el sistema electrónico que el Instituto establezca para tal efecto.

Artículo 55. La solicitud de acceso, rectificación, cancelación u oposición de los datos personales deberá contener, cuando menos, los requisitos siguientes:

I. Nombre del ente público a quien se dirija;

II. Nombre completo del titular y, en su caso, el 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, mismo que debe encontrarse dentro de la capital del Estado, o medio 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.

En el caso de solicitudes de acceso a datos personales, el titular o, en su caso, su representante legal deberá acreditar su identidad y personalidad, asimismo, deberá acreditarse la identidad antes de que el ente público proceda a la rectificación o cancelación.

En el caso de solicitudes de rectificación de datos personales, el titular 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 titular y ésta sea procedente.

En el caso de solicitudes de cancelación de datos personales, el titular deberá señalar las razones por las cuales considera que el tratamiento de los datos no se ajusta a lo dispuesto en la Ley.

Los medios por los cuales el solicitante podrá recibir notificaciones y acuerdos de trámite serán: correo electrónico, notificación personal en su domicilio o en la propia Unidad de Acceso a la Información Pública que corresponda. En el caso de que el solicitante no señale domicilio o algún medio de los autorizados por esta Ley para oír y recibir notificaciones, la prevención se notificará por lista que se fije en los estrados del ente público que corresponda.

El trámite de solicitud de acceso, rectificación, cancelación u oposición de datos de carácter personal es gratuito. No obstante, el titular deberá cubrir los costos de reproducción de los datos solicitados, en términos de lo previsto por el Código Financiero para el Estado y los respectivos Códigos Hacendarios Municipales, en materia de transparencia y acceso a la información.

El único medio por el cual el titular podrá recibir la información referente a los datos personales será la Unidad de Acceso a la Información Pública, y sin mayor formalidad que la de acreditar su identidad y cubrir los costos a que se refiere el apartado anterior.

Artículo 56. En caso de que el ente público determine que es procedente la rectificación o cancelación de los datos personales, deberá notificar al titular la procedencia de su petición, para que, dentro de los diez días hábiles siguientes, el titular o su representante legal acrediten fehacientemente su identidad ante la Unidad de Acceso a la Información Pública y se proceda a la rectificación o cancelación de los datos personales.

Artículo 57. En caso de que no proceda la solicitud, la Unidad de Acceso a la Información Pública deberá notificar al peticionario, de manera fundada y motivada, las razones por las cuales no procedió su petición. La respuesta deberá estar firmada por el titular de la referida Unidad de Acceso.

CAPÍTULO III
Del Recurso de Revisión

Artículo 58. El titular o su representante podrán interponer recurso de revisión ante el Instituto, en los términos previstos en el artículo 64 de la Ley de Transparencia y Acceso a la Información para el Estado y en los lineamientos generales para regular el procedimiento de substanciación del recurso de revisión.

Son impugnables por medio del recurso de revisión, las resoluciones que emita la Unidad de Acceso a la Información Pública del ente público, como resultado del ejercicio de los derechos de acceso, rectificación, cancelación y oposición de sus datos personales en posesión de entes públicos.

Lo anterior, sin perjuicio del derecho que les asiste a los titulares de interponer queja ante los órganos de control interno de los entes públicos.

Artículo 59. El Instituto 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.

Las resoluciones que emita el Instituto serán definitivas, inatacables y obligatorias para los entes públicos y los particulares; estos últimos podrán interponer el Juicio de Protección de Derechos Humanos ante la Sala Constitucional del Tribunal Superior de Justicia del Estado, de conformidad con el procedimiento establecido en la ley de la materia.

La autoridad judicial competente tendrá acceso a los sistemas de datos personales cuando resulte indispensable para resolver el asunto y hubiere sido ofrecido en juicio. Dicha información deberá ser mantenida con ese carácter y no estará disponible en el expediente.

TÍTULO QUINTO
Responsabilidades y Sanciones

CAPÍTULO I
De las Infracciones

Artículo 60. Constituyen infracciones a la presente Ley:

I. La omisión o irregularidad en la atención de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

II. Impedir, obstaculizar o negar el ejercicio de derechos a que se refiere la presente Ley;

III. Recabar datos de carácter personal sin proporcionar la información prevista en la presente Ley;

IV. Crear sistema de datos de carácter personal, sin la publicación previa en la Gaceta Oficial del estado;

V. Obtener datos sin el consentimiento expreso del titular cuando éste es requerido;

VI. Incumplir los principios y garantías previstos por la presente Ley;

VII. Transgredir las medidas de protección y confidencialidad a las que se refiere la presente Ley;

VIII. Omitir total o parcialmente el cumplimiento de las resoluciones emitidas por el Instituto, así como obstruir las funciones del mismo;

IX. Omitir o presentar de manera extemporánea los informes a que se refiere la presente Ley;

X. Obtener datos personales de manera engañosa o fraudulenta;

XI. Transmitir datos personales fuera de los casos permitidos, particularmente cuando la transmisión haya tenido por objeto obtener un lucro indebido;

XII. Impedir u obstaculizar la inspección ordenada por el Instituto o su instrucción de bloqueo de sistemas de datos personales;

XIII. Destruir, alterar, ceder datos personales, archivos o sistemas de datos personales sin autorización;

XIV. Incumplir la inmovilización de sistemas de datos personales ordenada por el Instituto; y

XV. El incumplimiento de cualquiera de las disposiciones contenidas en esta Ley.

Las infracciones a que se refiere este artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, serán resueltas por el Instituto, de conformidad con el procedimiento que se establezca mediante el Lineamiento respectivo, donde se cumplan las formalidades esenciales del procedimiento.

Lo anterior con independencia de las responsabilidades que se finquen mediante la aplicación de la Ley de Responsabilidades de los Servidores Públicos para el estado y las normas en esta materia contenidas en las leyes especiales que regulen a los entes públicos, según sea el caso, así como las de orden civil o penal que procedan y los procedimientos para el resarcimiento del daño ocasionado por el ente público.

Artículo 61. El Instituto denunciará ante las autoridades competentes cualquier conducta prevista en el artículo anterior y aportará las pruebas que considere pertinentes. Los órganos de control y fiscalización internos de los entes públicos entregarán semestralmente al Instituto un informe estadístico de los procedimientos administrativos iniciados con motivo del incumplimiento de la presente Ley y sus resultados.

CAPÍTULO II
De las Sanciones

Artículo 62. Las infracciones a que se refiere el artículo 60 de la presente Ley se sancionarán con multa de:

I. Cincuenta a quinientos días de salario mínimo general diario vigente en la zona económica que corresponda, en los casos de las fracciones I y II;

II. Trescientos a mil días de salario mínimo general diario vigente en la zona económica que corresponda, en los casos de las fracciones III a IX; y

III. Mil a diez mil días de salario mínimo general diario vigente en la zona económica que corresponda, en los casos de las fracciones X a XV.

Artículo 63. Las sanciones se impondrán tomando en cuenta los siguientes elementos:

I. La naturaleza de los derechos personales afectados;

II. El volumen de los tratamientos efectuados;

III. Los beneficios obtenidos;

IV. El grado de intencionalidad;

V. La reincidencia, si la hubiere; y

VI. Los daños y perjuicios causados.

En el caso de las fracciones IX a XII del artículo 60 de la presente Ley, el Instituto podrá, además, suspender o cancelar la operación del sistema de datos cuando existan circunstancias que atenten contra un grupo importante de titulares.

Las multas que imponga el Instituto tendrán el carácter de créditos fiscales y serán exigibles de inmediato, en los términos que para el efecto señalan el Código de Procedimientos Administrativos y el Código Financiero para el estado. La autoridad competente para el cobro es la Secretaría de Finanzas y Planeación del Gobierno del Estado, por conducto del área correspondiente, previa resolución certificada que le remita el Instituto, en la que haya fincado la multa.

Artículo 64. Las resoluciones en las que se impongan multas podrán ser impugnadas mediante el juicio contencioso administrativo ante el órgano jurisdiccional competente, sólo por cuanto respecta a la imposición de la sanción y su monto.

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

Primero. La presente Ley entrará en vigor al día siguiente de su publicación en la Gaceta Oficial del estado.

Segundo. Los entes públicos deberán notificar al Instituto, dentro de los ciento ochenta días hábiles después de la entrada en vigor de la presente Ley, la relación de sistemas de datos personales que posean para su registro.

Tercero. Los entes públicos, dentro del plazo de trescientos sesenta días naturales, contado a partir de la entrada en vigor de la presente Ley, deberán ajustar los sistemas de datos personales que posean, así como adecuar su normatividad interna.

Cuarto. Los entes públicos que a la entrada en vigor de la presente Ley no cuenten con un sistema de datos personales tendrán un plazo de trescientos sesenta días naturales para crear dicho sistema en términos de la presente Ley y demás normatividad que expida el Instituto.

Quinto. El Instituto deberá emitir los lineamientos a que se refiere la presente Ley en un plazo de ciento ochenta días naturales, posteriores a la entrada en vigor de la presente Ley.

Sexto. Se derogan el Capítulo Quinto del Título Primero de la Ley de Transparencia y Acceso a la Información para el Estado y todas las demás disposiciones que contravengan la presente Ley.

Dada en el salón de sesiones de la LXII Legislatura del Honorable Congreso del Estado, en la ciudad de Xalapa- Enríquez, Veracruz de Ignacio de la Llave, a los veintiséis días del mes de septiembre del año dos mil doce.

Eduardo Andrade Sánchez
Diputado presidente
Rúbrica.

Juan Carlos Castro Pérez
Diputado secretario
Rúbrica.

Por lo tanto, en atención a lo dispuesto por el artículo 49 fracción II de la Constitución Política del Estado, y en cumplimiento del oficio SG/001567 de los diputados Presidente y Secretario de la Sexagésima Segunda Legislatura del Honorable Congreso del Estado, mando se publique y se le dé cumplimiento. Residencia del Poder Ejecutivo Estatal, a los veintiséis días del mes de septiembre del año dos mil doce.

A t e n t a m e n t e

Sufragio efectivo. No reelección

Dr. Javier Duarte de Ochoa
Gobernador del Estado
Rúbrica.