LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL

Publicada en la Gaceta Oficial del Distrito Federal el 03 de Octubre de 2008

Última reforma publicada en la Gaceta Oficial del Distrito Federal
el 18 de diciembre de 2014

TÍTULO PRIMERO
DISPOSICIONES COMUNES PARA LOS ENTES PÚBLICOS

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

Bloqueo de datos personales: La identificación y reserva de datos personales con el fin de impedir su tratamiento;

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;

Datos personales: La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos;

Ente Público: La Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; El Tribunal de lo Contencioso Administrativo del Distrito Federal; El Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; la Jefatura de Gobierno del Distrito Federal; las Dependencias, Órganos Desconcentrados, Órganos Político Administrativos y Entidades de la Administración Pública del Distrito Federal; los

Órganos Autónomos por Ley; los partidos políticos, asociaciones y agrupaciones políticas; así como 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;

Instituto: El Instituto de Acceso a la Información Pública del Distrito Federal.

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

Oficina de 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;

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

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;

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;

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos, 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 ente público para prestarle servicios para el tratamiento de datos personales.

Artículo 3.- La interpretación de esta ley se realizará conforme a la Constitución Política de los Estados Unidos Mexicanos, la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales respectivos.

Artículo 4.- En todo lo no previsto en los procedimientos a que se refiere esta Ley, se aplicará de manera supletoria la Ley de Procedimiento Administrativo del Distrito Federal y, en su defecto, el Código de Procedimientos Civiles del Distrito Federal.

TITULO SEGUNDO
DE LA TUTELA DE DATOS PERSONALES

CAPÍTULO I
DE LOS PRINCIPIOS

Artículo 5.- Los sistemas de datos personales en posesión de los entes públicos se regirán por 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 ente público 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: Se refiere a la manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales.

Calidad de los Datos: Los datos personales recabados deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán ser los que respondan con veracidad a la situación actual del interesado.

Confidencialidad: Consiste en garantizar que exclusivamente la persona interesada puede acceder a los datos personales o, en caso, el responsable o el usuario del sistema de datos personales para su tratamiento, así como el deber de secrecía del responsable del sistema de datos personales, así como de los usuarios.

Los instrumentos jurídicos que correspondan a la contratación de servicios del responsable 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, así como las penas convencionales

por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables.

Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el ente público con el titular de los datos personales, así como después de finalizada la relación laboral entre el ente público y el responsable del sistema de datos personales o los usuarios.

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.

Seguridad: Consiste en 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, mediante los procedimientos que para tal efecto se establezcan.

Disponibilidad: Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado.

Temporalidad: Los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados. Queda exceptuado el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación. Únicamente podrán ser conservados de manera integra, permanente y sujetos a tratamiento los datos personales con fines históricos.

CAPÍTULO II
DE LOS SISTEMAS DE DATOS PERSONALES

Artículo 6.- Corresponde a cada ente público determinar, a través de su titular o, en su caso, del órgano competente, la creación, modificación o supresión de sistemas de datos personales, conforme a su respectivo ámbito de competencia.

Artículo 7.- La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:

I. Cada ente público deberá publicar en la Gaceta Oficial del Distrito Federal la creación, modificación o supresión de su sistema de datos personales;

II. En caso de creación o modificación de sistemas de datos personales, se deberá indicar por lo menos:

a) La finalidad del sistema de datos personales y los usos previstos para el mismo;

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

c) El procedimiento de recolección de los datos de carácter personal;

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

e) De la cesión de las que pueden ser objeto los datos;

f) Las instancias responsables del tratamiento del sistema de datos personales;

g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición; y

h) El nivel de protección exigible.

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

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

Artículo 8.- Los sistemas de datos personales en posesión de los entes públicos deberán inscribirse en el registro que al efecto habilite el Instituto. El registro debe comprender como mínimo la información siguiente:

I. Nombre y cargo del responsable y de los usuarios;

II. Finalidad del sistema;

III. Naturaleza de los datos personales contenidos en cada sistema;

IV. Forma de recolección y actualización de datos;

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

VI. Modo de interrelacionar la información registrada;

VII. Tiempo de conservación de los datos, y

VIII. Medidas de seguridad.

Artículo 9.- Cuando los entes públicos recaben datos personales deberán informar previamente a los interesados de forma expresa, precisa e inequívoca lo siguiente:

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 interesado, 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; y

VI. Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

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.

En caso de que los datos de carácter personal no hayan sido obtenidos 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 de lo previsto en las fracciones I, IV y V del presente artículo.

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 10.- Ninguna persona está obligada a proporcionar datos personales considerados como sensibles, tal y como son: el origen étnico o racial,

características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual.

Queda prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar los datos personales señalados en el párrafo 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.

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

Artículo 11.- 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 12.- 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 III
DE LAS MEDIDAS DE SEGURIDAD

Artículo 13.- Los entes públicos establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de cada sistema 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 sistemas.

Dichas 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.

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 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 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 30días hábiles siguientes a la fecha en que se efectuó.

Artículo 14.- El ente público responsable de la tutela y tratamiento del sistema de datos personales, adoptará las medidas de seguridad, conforme a lo siguiente:

A. Tipos de seguridad:

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

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

III. **De desarrollo y aplicaciones.-** Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a

seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas;

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

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

B. Niveles de seguridad:

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

a) Documento de seguridad;

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

c) Registro de incidencias;

d) Identificación y autentificación;

e) Control de acceso;

f) Gestión de soportes, y

g) Copias de respaldo y recuperación.

II. **Medio.-** Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas, delitos, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos.[1]

a) Responsable de seguridad;

b) Auditoria;

[1] *Reforma publicada en GODF el 18 de diciembre 2014*

c) Control de acceso físico; y

d) Pruebas con datos reales.

III. **Alto.-** Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes 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) Distribución de soportes;

b) Registro de acceso; y

c) Telecomunicaciones.

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

Artículo 15.- Las medidas de seguridad a las que se refiere el artículo anterior 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.

CAPÍTULO IV
DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 16.- El tratamiento de los datos personales, requerirá el consentimiento inequívoco, expreso y por escrito del interesado, salvo en los casos y excepciones siguientes:

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

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.

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 oficina de 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 17.- 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 la autoridad competente de conformidad por la Ley Federal de Responsabilidades de los Servidores Públicos.

Artículo 18.- 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 Distrito Federal y demás normas que de ellas deriven. El tratamiento y cesión a 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 personales queda limitado estrictamente a los fines específicos de cada caso.

Artículo 19.- 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 deberá establecer el plazo de conservación por el usuario, al término del cual los datos deberán ser devueltos en su totalidad al ente público, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

Artículo 20.- En caso de que los destinatarios de los datos sean instituciones de 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 V
DE LAS OBLIGACIONES DE LOS ENTES PÚBLICOS

Artículo 21.- El titular del ente público designará al responsable de los sistemas de datos personales, mismo que deberá:

I. Cumplir con las políticas y lineamientos así como las 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 correspondiente 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 interesado al momento de recabar sus datos personales, 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. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;

VII. 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;

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 interesado, siempre y cuando se cuente con el documento que avale la actualización de dichos datos. Lo anterior, sin perjuicio del derecho del interesado para solicitar la rectificación o cancelación de los datos personales que le conciernen;

IX. Establecer 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. Resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos de las personas;

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

XIII. 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;

XIV. Coordinar y supervisar la adopción de las medidas de seguridad a que se encuentren sometidos los sistemas de datos personales de acuerdo con la normativa vigente;

XV. 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

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

Artículo 22.- 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
DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO ÚNICO
DEL INSTITUTO Y SUS ATRIBUCIONES

Artículo 23.- El Instituto de Acceso a la Información Pública del Distrito Federal 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 24.- El Instituto 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;

IV. Llevar a cabo 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 esta Ley;

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. Dicha evaluación se incluirá en el informe que de conformidad con el artículo 74 de la Ley de Transparencia y Acceso a la información pública presenta el Instituto a la Asamblea Legislativa del Distrito Federal y deberá incluir por lo menos:

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, 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. Investigar, 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 del Distrito Federal;

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 interesados 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 establezca esta Ley, y demás ordenamientos aplicables.

Artículo 25.- 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 del Distrito Federal, sobre los sistemas y las medidas de seguridad que precisa la tutela de los datos personales de cada ente público.

TÍTULO CUARTO
DE LOS DERECHOS Y DEL PROCEDIMIENTO PARA SU EJERCICIO

CAPÍTULO I
DERECHOS EN MATERIA DE DATOS PERSONALES

Artículo 26.- Todas las personas, previa identificación mediante documento oficial, contarán 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 a cualquiera de los derechos previstos en la presente ley, deberá ser proporcionada en forma legible e inteligible, pudiendo suministrase, a opción del interesado, por escrito o mediante consulta directa.

Artículo 27.- 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 28.- Procederá el derecho de rectificación de datos del interesado, en los sistemas de datos personales, cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos, siempre y cuando no resulte imposible o exija esfuerzos desproporcionados.

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 29.- 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 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 30.- El interesado 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 interesado.

Artículo 31.- 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, quién deberá también proceder a la rectificación o cancelación de los mismos.

CAPÍTULO II
DEL PROCEDIMIENTO

Artículo 32.- La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que se formule a los entes públicos se sujetarán al procedimiento establecido en el presente capítulo.

Sin perjuicio de lo que dispongan otras leyes, sólo el interesado o su representante legal, previa acreditación de su identidad, podrán solicitar al ente público, a través de la oficina de información pública competente, 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.

La oficina de 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 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 párrafo anterior, podrá ser ampliado una única vez, por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Si al ser presentada la solicitud no es precisa o no contiene todos los datos requeridos, en ese momento el Ente Público, en caso de ser solicitud verbal, deberá ayudar al solicitante a subsanar las deficiencias. Si los detalles proporcionados por el solicitante no bastan para localizar los datos personales o son erróneos, la oficina de información pública del ente público podrá prevenir, 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 ente público 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 titular de la oficina de información pública y por el responsable del sistema de datos personales del ente público.

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 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, el titular de la oficina de información pública y el responsable del sistema de datos personales del ente público.

Artículo 33.- La solicitud de acceso, rectificación, cancelación u oposición de datos personales, se deberá presentar ante la oficina de información pública del ente público que el interesado considere que está procesando información de su persona. El procedimiento de acceso, rectificación, cancelación u oposición de datos personales, iniciará con la presentación de una solicitud en cualquiera de las siguientes modalidades:

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

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

III. Por correo electrónico, será la que realiza el interesado a través de una dirección electrónica y sea enviada a la dirección de correo electrónico asignada a la oficina de información pública del ente público;

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

V. Por vía telefónica, en términos de los lineamientos que expida el Instituto.

Artículo 34.- 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 interesado, 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 se debe encontrar dentro del Distrito Federal, 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 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 ente público proceda a la rectificación o cancelación.

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.

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 oficina de 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 de la Oficina de Información Pública del Ente Público que corresponda.

El único medio por el cual el interesado podrá recibir la información referente a los datos personales será la oficina de información pública, y sin mayor formalidad que la de acreditar su identidad y cubrir los costos de conformidad con la presente Ley y el Código Financiero del Distrito Federal.

El Instituto y los entes públicos contarán con la infraestructura y los medios tecnológicos necesarios para garantizar el efectivo acceso a la información de las personas con discapacidad.

Artículo 35.- Presentada la solicitud de acceso, rectificación, cancelación u oposición de datos personales, la oficina de información pública del ente público, 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, de no ser así se prevendrá al interesado, tal y como lo señala el artículo 32 de la presente Ley. 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 la respuesta que corresponda;

III. La unidad administrativa informará a la oficina de información pública de la existencia de la información solicitada. En caso de inexistencia, se procederá de conformidad con lo previsto por el artículo 32 para que la oficina de información pública a su vez realice una nueva búsqueda en otra área o unidad administrativa.

En la respuesta, la oficina de información pública, señalará el costo que por concepto de reproducción deberá pagar el solicitante en los términos del Código Financiero del Distrito Federal;

IV. La oficina de información pública, notificará en el domicilio o a través del medio señalado para tal efecto, la existencia de una respuesta para que el interesado o su representante legal pasen a recogerla a la oficina de información pública;

V. 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; y

VI. Previa exhibición del original del documento con el que acreditó su identidad el interesado o su representante legal, se hará entrega de la información requerida.

En caso de que el ente público determine que es procedente la rectificación o cancelación de los datos personales, deberá notificar al interesado la procedencia de su petición, para que, dentro de los 10 días hábiles siguientes, el interesado o su representante legal acrediten fehacientemente su identidad ante la oficina de información pública y se proceda a la rectificación o cancelación de los datos personales.

Artículo 36.- En caso de que no proceda la solicitud, la oficina de 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 oficina de información pública y por el responsable del sistema de datos personales, pudiendo recaer dichas funciones en la misma persona.

Artículo 37.- El trámite de solicitud de acceso, rectificación, cancelación u oposición de datos de carácter personal 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 del Distrito Federal.

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 Entes Públicos deberán esforzarse por reducir al máximo, los costos de entrega de información.

CAPÍTULO III
DEL RECURSO DE REVISIÓN

Artículo 38.- Podrá interponer recurso de revisión ante el Instituto, el interesado que se considere agraviado por la resolución definitiva, que recaiga a su solicitud de acceso, rectificación, cancelación u oposición o ante la omisión de la respuesta. Para este efecto, las oficinas de información pública al dar respuesta a las solicitudes, orientarán al particular sobre su derecho de interponer el recurso de revisión y el modo y plazo para hacerlo.

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

Artículo 39.- 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. En contra de las resoluciones del Instituto el particular podrá interponer juicio de amparo. La autoridad judicial competente tendrá acceso a los sistemas de datos personales cuando resulte indispensable para resolver el asunto y hubiera sido ofrecida en juicio. Dicha información deberá ser mantenida con ese carácter y no estará disponible en el expediente.

Artículo 40.- El recurso de revisión será tramitado de conformidad con los términos, plazos y requisitos señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal. Igualmente, el recurrente podrá interponer el recurso de revocación, que será sustanciado en los términos que establezca la propia Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y el Reglamento Interior del Instituto.

TÍTULO QUINTO
DE LAS RESPONSABILIDADES

CAPÍTULO ÚNICO
DE LAS INFRACCIONES

Artículo 41.- 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 Distrito Federal;

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

VI. Incumplir los principios 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 realizadas 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, y

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

XIV. Incumplir con 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, será sancionada en términos de la Ley de Federal de Responsabilidades de los Servidores Públicos, siendo independientes de las de orden civil o penal que procedan, así como los procedimientos para el resarcimiento del daño ocasionado por el ente público.

Artículo 42.- 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. Esta información será incorporada al informe anual del Instituto.

Dicha resolución se comunicará al Ente Público y al responsable del sistema de datos personales y, en su caso, a los interesados de los datos personales que resultaren afectados.

Lo anterior sin perjuicio de las responsabilidades penales o civiles que pudieran derivarse.

TRANSITORIOS

PRIMERO. El presente decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial del Distrito Federal. Publíquese en el Diario de la Federación para su mayor difusión.

SEGUNDO. Publíquese en la Gaceta Oficial del Distrito Federal para su debida observancia y aplicación.

TERCERO. Los entes públicos deberán notificar al Instituto, treinta días hábiles después de la entrada en vigor de la presente Ley, la relación de Sistemas de Datos Personales que posean para su registro.

CUARTO. El documento en el que se establezcan los niveles de seguridad a las que se refiere el capítulo III del Título II de la presente Ley, deberá ser emitido por los entes públicos dentro de los sesenta días hábiles posteriores a la entrada en vigor de la Ley, mismo que deberá ser remitido al Instituto para su registro dentro del mismo plazo.

PRIMERO. Publíquese en la Gaceta Oficial del Distrito Federal.

SEGUNDO. El presente Decreto entrará en vigor en los términos establecidos en la Declaratoria de la Incorporación del Sistema Procesal Penal Acusatorio y del Código Nacional de Procedimientos Penales al orden jurídico del Distrito Federal, publicada en la Gaceta Oficial el día 20 de agosto del presente año, así como su Fe de Erratas y Aclaratoria de Fe de Erratas, publicadas en la Gaceta Oficial, los días 21 y 22 de agosto del 2014.

TERCERO. Los asuntos iniciados con anterioridad a la entrada en vigor del presente decreto, se tramitarán conforme a las disposiciones anteriores, que le sean aplicables.

CUARTO. La reforma al Código de Instituciones y Procedimientos Electorales del Distrito Federal prevista en el presente Decreto, entrará en vigor al día siguiente a aquél en que concluya el proceso electoral local de 2014-2015 en el Distrito Federal.