

DECRETO

La LX Legislatura del Congreso del Estado de Campeche decreta:

NÚMERO 231

ARTÍCULO PRIMERO.- Se expide la Ley de Protección de Datos Personales del Estado de Campeche y sus Municipios, para quedar como sigue:

LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE CAMPECHE Y SUS MUNICIPIOS

TÍTULO PRIMERO

DISPOSICIONES COMUNES PARA LOS ENTES PÚBLICOS

CAPÍTULO ÚNICO

DISPOSICIONES GENERALES

Artículo 1.- La presente Ley es de orden público e interés social y tiene por objeto proteger y garantizar los datos personales en poder de los Entes Públicos del Estado.

Artículo 2.- Esta Ley será aplicable a los datos personales que sean registrados en cualquier soporte físico, que permita su tratamiento por parte de las entidades del sector público.

Se exceptúan de su aplicación:

- I. Los archivos que sean considerados como clasificados por la ley; y
- II. Los archivos establecidos para investigaciones penales. En este caso, el responsable del archivo deberá comunicar la existencia del mismo a la Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, indicando sus características generales y su finalidad.

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

- I. **Archivo:** El conjunto de datos de carácter personal, correspondientes a un grupo de personas, independientemente de su forma de creación, almacenamiento, tratamiento o uso;
- II. **Archivo de acceso público:** El archivo que puede ser consultado por cualquier persona que no esté impedida por una disposición legal, ya sea gratuitamente o mediante el pago de los derechos correspondientes;

III. **Cesión de datos:** La comunicación o transmisión de datos hacia una persona distinta del interesado;

IV. **Comisión:** La Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche, autoridad encargada de la aplicación del presente ordenamiento;

V. **Consentimiento:** La manifestación expresa, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de datos personales de los que es titular;

VI. **Datos personales:** La información concerniente a una persona física identificada e identificable, relativa a su origen racial o étnico, o que este referida a sus características físicas, morales o emocionales, a su vida afectiva o familiar, domicilio, número telefónico, patrimonio, ideología, creencias o convicciones religiosas o filosóficas, su estado de salud físico o mental, sus preferencias sexuales, datos biométricos como la huella digital, datos sobre el DNA de las personas, claves informáticas o cibernéticas, códigos personales encriptados u otros análogos que se encuentren vinculados a su intimidad, entre otros.

VII. **Encargado del tratamiento:** El Ente Público que realice el tratamiento de datos por cuenta y con autorización del titular de los mismos;

VIII. **Interesado o afectado:** La persona física cuyos datos de carácter personal se incorporen al archivo o sistema;

IX. **Ley:** El presente ordenamiento;

X. **Proceso de disociación:** El tratamiento de los datos personales de modo que los datos resultantes no puedan ser relacionados directamente con ninguna persona identificable;

XI. **Responsable del archivo o sistema:** La persona física o moral, pública, encargada del tratamiento de los datos del archivo o sistema;

XII. **Representante Legal:** La persona autorizada por el titular de los datos para tener acceso a los mismos en su nombre y representación. La representación legal sólo se podrá acreditar mediante poder notarial.

XIII. **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;

XIV. **Sujetos obligados:** Los Entes Públicos a que se refiere la fracción IV del artículo 4 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.

XV. **Tratamiento de datos:** Las operaciones y procesos, automatizados o manuales, relacionados con la recolección, captura, conservación, proceso, transmisión, interrelación, combinación, control y otros manejos de los datos;

XVI. **Unidad de Acceso:** La unidad administrativa de los sujetos obligados receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en la presente Ley y en los lineamientos que expida la Comisión.

XVII. **Usuario:** Aquel autorizado por el Ente Público para prestarle servicios para el tratamiento de los sistemas de datos personales.

TÍTULO SEGUNDO

DE LA TUTELA DE LOS DATOS PERSONALES

CAPÍTULO I

DE LOS PRINCIPIOS

Artículo 4.- Los sistemas de datos personales en posesión de los Entes Públicos se registrarán por los principios siguientes:

Licitud: Consiste en que la posesión y tratamiento de los sistemas de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada Ente Público y deberán obtenerse a través de los 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 los datos personales con fines históricos, estadísticos o científicos.

Consentimiento: Se refiere a la manifestación de la 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 el titular o su representante legal pueden acceder a los datos personales o, en su caso, el responsable o el usuario del sistema de datos personales para su tratamiento, quienes deberán observar el deber de secrecía.

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 la 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 se podrán transmitir 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 5.- Corresponde a cada Ente Público determinar, a través de su titular o, en su caso, del órgano competente, la creación, modificación o supresión de los sistemas de datos personales, conforme a su respectivo ámbito de competencia.

Artículo 6.- La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:

I. Los archivos que contengan datos personales en posesión de los Entes Públicos deberán ser enlistados y dichas listas remitidas a la Comisión la cual deberá asegurarse que:

- a) Los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida al momento de su recolección;
- b) Ninguno de esos datos sea utilizado o revelado sin su consentimiento, con un propósito incompatible al que se haya especificado; y
- c) El período de conservación de los datos personales sea el necesario para alcanzar la finalidad con que se hayan recolectado y registrado.

Cada Ente Público deberá publicar en su página de Internet la creación, modificación o supresión de sus sistemas de datos personales, dando aviso a la Comisión en los plazos y mediante los procedimientos establecidos en esta Ley y en los lineamientos que para tal efecto emita dicho organismo.

II. En caso de creación o modificación de los 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 la que puedan 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 7.- 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,

la finalidad de la obtención de éstos y 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 8.- 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 preferencias sexuales.

Queda prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar los datos señalados en el párrafo anterior y sólo pueden ser tratados cuando medien razones de interés general, cuando 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, no será necesario el procedimiento de disociación.

Artículo 9.- Los archivos o sistemas creados con fines administrativos por los Entes Públicos, 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 de seguridad pública, 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, prevención o persecución de delitos, debiendo ser almacenados en sistemas específicos, establecidos para tal 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, podrá realizarse exclusivamente en los supuestos en que sean absolutamente necesarios para los fines de una investigación concreta, sin perjuicio del control de legalidad en la actuación administrativa o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales.

Los datos personales recabados con estos fines se cancelarán cuando ya 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 10.- Los responsables de los sistemas de datos personales con fines de seguridad pública, para la prevención de conductas delictivas o en materia tributaria, podrán negar el acceso, rectificación, cancelación y oposición de los mismos, en función de los peligros que pudieran derivarse para la seguridad o la defensa del Estado, 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.

Artículo 11.- La cesión de los datos de carácter personal o su comunicación a terceros, se regirá por lo siguiente:

I. Toda cesión o comunicación a terceros deberá contar con el consentimiento expreso del interesado, excepto cuando:

- a) La cesión haya sido autorizada en una ley;
- b) Se trate de datos disponibles en fuentes de acceso público;
- c) Sea necesario y esté previsto como parte de una relación jurídica;
- d) Esté dirigida a las autoridades de seguridad pública o penales y cuente con autorización judicial;
- e) Se trate de transferencias entre administraciones públicas;
- f) Sea transferida para fines históricos, estadísticos o científicos; y
- g) Se trate de datos sobre la salud y sean necesarios para atender una urgencia o para realizar estudios epidemiológicos;

II. El receptor de datos de carácter personal se obliga a acatar las disposiciones de la presente Ley;

III. Cuando la comunicación a terceros resulte de la prestación por parte de un tercero de servicios al responsable del archivo, el tercero en cuestión se considerará obligado en términos de la presente Ley, en las mismas condiciones que el responsable del archivo; y

IV. También queda obligado a acatar las disposiciones de la presente Ley, quien obtenga los datos en virtud de liquidación, fusión, escisión u otro cambio, en el caso de que los datos provengan de personas morales, o por herencia, en el caso de provenir de personas físicas.

CAPÍTULO III

DE LAS MEDIDAS DE SEGURIDAD

Artículo 12.- 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 preservar el pleno ejercicio de los derechos tutelados en la presente Ley, frente a su alteración, pérdida, transmisión y acceso no autorizado, de conformidad con el 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 a la Comisión 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 intervenga en el tratamiento de los datos personales con el carácter de responsable del sistema 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 a la Comisión dentro de los treinta días hábiles siguientes a la fecha en que se efectuó.

Artículo 13.- 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 autenticación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función;

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

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

V. **De comunicaciones y redes.-** Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a

un dominio 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 autenticación;
- e) Control de acceso;
- f) Gestión de soportes, y
- g) Copias de respaldo y recuperación.

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

- a) Responsable de seguridad;
- b) Auditoria;
- 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 14.- 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 a la Comisión, para su registro, el nivel de seguridad aplicable.

CAPÍTULO IV

DEL TRATAMIENTO DE DATOS PERSONALES

Artículo 15.- El tratamiento de los datos personales, requerirá del 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 prevista 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, con la condición de 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 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, debiendo responder solidariamente por la inobservancia de las mismas.

Artículo 16.- 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, la Comisión podrá requerir a los responsables de los sistemas de datos personales, la suspensión en la utilización o cesión de los datos. Si el requerimiento fuere desatendido, mediante resolución fundada y motivada, la Comisión podrá bloquear tales sistemas, de conformidad con el procedimiento que al efecto se establezca. El incumplimiento a la inmovilización ordenada por la Comisión será sancionado por la autoridad competente de conformidad con la Ley Reglamentaria del Capítulo XVII de la Constitución Política del Estado de Campeche.

Artículo 17.- 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 de Campeche y demás normas que de ellas deriven. El tratamiento y cesión de esta información obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico- asistencial, de manera tal que se mantenga la confidencialidad de los mismos, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación científica, de salud pública o con fines judiciales, en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales. El acceso a los datos y documentos relacionados con la salud de las personas queda limitado estrictamente a los fines específicos de cada caso.

Artículo 18.- 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 19.- 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.

TÍTULO TERCERO

DEL EJERCICIO DE LOS DERECHOS EN MATERIA DE DATOS PERSONALES

CAPÍTULO I

DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN U OPOSICIÓN

Artículo 20.- 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 el ejercicio de alguno de ellos no es requisito previo o impedimento para 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 suministrarse, a opción del interesado, por escrito o mediante consulta directa.

Artículo 21.- 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 22.- 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 23.- El interesado tendrá derecho a solicitar la cancelación de sus datos cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en los lineamientos emitidos por la Comisión, o cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de los 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 24.- 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 25.- 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 26.- La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que se formulen a los Entes Públicos se sujetará al procedimiento establecido en el presente Capítulo y a los lineamientos que al efecto emita la Comisión.

Artículo 27.- 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 Unidad de Acceso 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 en poder del sujeto obligado, mediante el cumplimiento de los siguientes requisitos:

- I. Solicitud por escrito en la que se exprese el nombre, domicilio u otro medio para recibir notificaciones y los datos personales cuyo acceso, cancelación u oposición se requieren o la descripción clara de las correcciones a realizarse, acompañando los documentos que motiven su solicitud, en su caso;
- II. Identificación oficial del solicitante;
- III. Firma o huella digital; y
- IV. 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 ningún caso los datos personales solicitados o las correcciones realizadas podrán enviarse por medios electrónicos o entregarse en dispositivos magnéticos u ópticos.

Artículo 28.- La Unidad de Acceso correspondiente deberá notificar al solicitante en el domicilio o medio electrónico señalado para tales efectos, en un plazo máximo de veinte días hábiles contados a partir del día hábil siguiente a la presentación de la solicitud, la determinación adoptada en relación con su petición, a efecto de que, de resultar procedente, se haga efectiva la misma dentro de los diez días hábiles siguientes a la fecha de la citada notificación, previo pago de los derechos correspondientes, en su caso.

El plazo de veinte días hábiles referido en el párrafo anterior, podrá ser ampliado por una sola vez, por un período igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Artículo 29.- Cuando la solicitud resulte confusa, sea omisa en contener los detalles necesarios para la localización de los datos personales o no satisfaga alguno de los requisitos previstos en el presente Capítulo, la Unidad de Acceso procederá, dentro de los tres días siguientes a la recepción de la solicitud, a requerir al interesado para que, en el plazo de cinco días hábiles contados a partir del día siguiente del requerimiento, haga las aclaraciones pertinentes o subsane las omisiones en que haya incurrido. De no recibir la aclaración correspondiente, la solicitud se tendrá como no interpuesta.

Este requerimiento interrumpe el plazo establecido para dar respuesta a las solicitudes por parte de la Unidad de Acceso.

Artículo 30.- En el supuesto de que los datos personales a que se refiere la solicitud obren en los sistemas relativos 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 Unidad de Acceso 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 una resolución en la que se indiquen los sistemas de datos personales en los que se realizó la búsqueda. Dicha resolución deberá estar firmada por el titular de la Unidad de Acceso y por el responsable del sistema de datos personales del Ente Público.

Artículo 31.- Las solicitudes de acceso, rectificación, cancelación u oposición de datos personales, podrán ser presentadas por los medios siguientes, a elección del interesado o de su representante legal:

I. Personalmente, ante la Unidad de Acceso correspondiente, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;

II. Por correo electrónico, a la dirección de correo electrónico asignada a la Unidad de Acceso del Ente Público; y

III. Por el sistema electrónico que la Comisión o el Ente Público establezcan para tal efecto.

Artículo 32.- 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 de los datos.

Artículo 33.- 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.

Artículo 34.- 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.

Artículo 35.- Los medios por los cuales el solicitante podrá recibir notificaciones serán: correo electrónico, sistema electrónico, notificación personal en su domicilio o en la Unidad de Acceso que corresponda. Si el interesado fuere omiso en señalar domicilio o dirección de correo electrónico, las notificaciones se le harán fijando una copia autorizada de la providencia o resolución en los estrados o cartelera de avisos de la Unidad de Acceso que corresponda.

El único medio por medio del cual el interesado o su representante legal podrán recibir la información referente a los datos personales será la Unidad de Acceso del Ente Público, sin mayor formalidad que la de acreditar su identidad y cubrir los costos de conformidad con la presente Ley y la legislación hacendaria del Estado; el titular también podrá recibir la

información referente a sus datos personales por medio de correo certificado con notificación, previo pago de los derechos correspondientes.

El Instituto y los Entes Públicos contarán con la infraestructura y los medios tecnológicos necesarios para garantizar el efectivo acceso, rectificación, cancelación u oposición de los datos personales de los individuos con discapacidad.

Artículo 36.- La Comisión deberá expedir los lineamientos que establezcan de manera detallada los procedimientos a que se sujetará la recepción, procesamiento, resolución y notificación de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

Artículo 37.- El trámite de las solicitudes 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 la legislación hacendaria del Estado.

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 la información.

CAPÍTULO III

DEL RECURSO DE REVISIÓN

Artículo 38.- Podrá interponer recurso de revisión ante la Comisión el interesado que se considere agraviado por la resolución que recaiga a su solicitud de acceso, rectificación, cancelación u oposición o ante la omisión de la respuesta. Para este efecto, las Unidades de Acceso 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.

Artículo 39.- La Comisión 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 la Comisión podrán impugnarlas los particulares ante la Sala Administrativa del Tribunal Superior de Justicia del Estado, mediante el juicio de nulidad previsto en el Código de Procedimientos Contencioso-Administrativos del Estado; y las Unidades de Acceso ante el Pleno del citado Tribunal, conforme a las disposiciones establecidas en dicho Código para la tramitación del recurso de revisión. En este último caso la Comisión no podrá requerir la ejecución o cumplimiento de su resolución hasta en tanto ésta no haya sido confirmada por el Tribunal Pleno.

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 plazos, procedimientos y requisitos señalados en la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.

TÍTULO CUARTO

DE LA AUTORIDAD RESPONSABLE DEL CONTROL Y VIGILANCIA

CAPÍTULO ÚNICO

DE LA COMISIÓN

Artículo 41.- La Comisión será el organismo responsable de la tutela de los derechos consignados en la presente Ley.

Artículo 42.- La Comisión tendrá las atribuciones siguientes:

- I. Vigilar el cumplimiento de esta Ley, particularmente en lo relativo a los derechos de datos personales;
- II. Emitir los lineamientos para el ejercicio de los derechos en materia de acceso, rectificación, cancelación u oposición de datos personales, incluyendo los formatos correspondientes;
- III. Conocer y resolver los recursos que se interpongan contra los actos y resoluciones emanados de los Entes Públicos, en los términos previstos en esta Ley y en la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche;
- IV. Evaluar la actuación de los Entes Públicos en materia de protección de datos personales, mediante la práctica de visitas de inspección, emitiendo las recomendaciones o resoluciones a que hubiere lugar;

V. Informar a los ciudadanos acerca de sus derechos de acceso, rectificación, cancelación u oposición de datos de carácter personal y asesorarles en la materia;

VI. Elaborar y mantener actualizado el listado de los sistemas de datos personales en poder de los Entes Públicos, así como el registro de los niveles de seguridad establecidos por los mismos;

VII. Difundir y promover el ejercicio de los derechos plasmados en la presente Ley; y

VIII. Las demás que sean necesarias para el cumplimiento de las anteriores atribuciones.

Artículo 43.- En el Informe Anual que rinde la Comisión al H. Congreso del Estado, se deberá detallar la información concerniente a las solicitudes recibidas y tramitadas por los Entes Públicos en materia de acceso, rectificación, cancelación y oposición de datos personales, así como el estado de las impugnaciones recaídas a las mismas.

TÍTULO QUINTO

DE LAS RESPONSABILIDADES

CAPÍTULO ÚNICO

DE LAS INFRACCIONES Y SANCIONES

Artículo 44.- Son infracciones a la presente Ley:

I. No atender las solicitudes que presenten los interesados para el acceso, rectificación, cancelación u oposición de sus datos personales, cuando éstas procedan legalmente;

II. Recabar datos de carácter personal sin proporcionar la información especificada en la presente Ley;

III. No remitir a la Comisión los niveles de seguridad establecidos para la protección de los sistemas de datos personales en poder de los Entes Públicos;

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

V. Incumplir los principios que rigen a los sistemas de datos personales, definidos en la presente Ley;

VI. Impedir, obstaculizar o negar el ejercicio de los derechos de los interesados en materia de datos personales establecidos en la presente Ley;

VII. La violación del secreto de los datos;

VIII. No remitir los listados de los sistemas de datos personales establecidas en la presente Ley a la Comisión, obstruir las funciones de la misma y no acatar sus disposiciones;

IX. La obtención de datos personales de manera engañosa o fraudulenta;

X. Tratar los datos de manera ilegítima; y

XI. La violación de la secrecía en el caso de los archivos de carácter policial, fiscal o de salud.

Artículo 45.- Las infracciones a que se refiere el artículo anterior o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada en términos de la Ley Reglamentaria del Capítulo XVII de la Constitución Política de los Estados Unidos Mexicanos, 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 46.- La Comisión denunciará ante las autoridades competentes cualquier conducta prevista en el presente Capítulo y aportará las pruebas que considere pertinentes. Los órganos internos de control de los Entes Públicos entregarán semestralmente a la Comisión un informe estadístico de los procedimientos administrativos iniciados con motivo del incumplimiento de la presente Ley y sus resultados. Esta información será incorporada al Informe Anual de la Comisión.

ARTÍCULO SEGUNDO.- Se deroga el Capítulo Séptimo “De la Protección de Datos Personales” del Título Primero “Disposiciones Comunes para los Sujetos Obligados”, artículos del 31 al 38, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, así como la fracción V del Artículo 3 del mismo ordenamiento jurídico.

TRANSITORIOS

PRIMERO.- El presente decreto entrará en vigor a los quince días siguientes de su publicación en el Periódico Oficial del Estado.

SEGUNDO.- Los lineamientos para el acceso, rectificación, cancelación y oposición de los datos personales en poder de los entes públicos, serán actualizados o expedidos por la Comisión a más tardar dentro de los noventa días naturales siguientes a la entrada en vigor del presente decreto.

TERCERO.- Las solicitudes que antes de la entrada en vigor de la presente Ley, hayan presentado los particulares ante las Unidades de Acceso de los Entes Públicos, para que les proporcionen, modifiquen o cancelen sus datos personales que obren en archivo o sistema determinado, deberán concluir observándose las disposiciones contenidas en la Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.

CUARTO.- Los entes públicos deberán notificar a la Comisión, sesenta días después de la entrada en vigor de la presente Ley, la relación de los Sistemas de Datos Personales que posean para su registro.

QUINTO.- El documento en el que se establezcan los niveles de seguridad a los que se refiere el Capítulo III del Título Segundo de la presente Ley, deberá ser emitido por los entes públicos dentro de los sesenta días posteriores a la entrada en vigor de la presente Ley, mismo que deberá ser remitido a la Comisión para su registro dentro del mismo plazo.

SEXTO.- Se derogan todas las disposiciones legales y reglamentarias en lo que se opongan al contenido del presente decreto.

Dado en el Salón de Sesiones del Palacio Legislativo, en la ciudad de San Francisco de Campeche, Campeche, a los diecinueve días del mes de junio del año dos mil doce.

C. Gloria del Carmen Gutiérrez Ocampo.

Diputada Presidenta.

C. Silvia María Avilés Rivera.

Diputada Secretaria.

C. José Benedicto Barony Blanquet.

Diputado Secretario.