

NORMAS PARA LA PROTECCIÓN, TRATAMIENTO, SEGURIDAD Y RESGUARDO DE LOS DATOS PERSONALES EN POSESIÓN DE LOS ENTES OBLIGADOS

CAPÍTULO I Disposiciones Generales

PRIMERA. Las presentes disposiciones son de observancia general y obligatoria para los entes obligados y tienen por objeto establecer las normas, principios y procedimientos que garanticen a los interesados el derecho a decidir sobre el uso y destino de sus datos personales, el adecuado tratamiento de los mismos y su transmisión lícita, en los términos del artículo 17 Bis de la Constitución del Estado y los artículos 2º, 12 y demás relativos de la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí.

SEGUNDA. Estas disposiciones son aplicables a los datos de carácter personal registrados en cualquier soporte, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior que se de a los datos por los entes obligados.

TERCERA. La interpretación y aplicación de estas disposiciones se hará conforme a los principios que se establecen en el artículo 10 de la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí.

CUARTA. Para efectos de las presentes disposiciones, en adición a lo preceptuado por el artículo 3º de la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí, se entenderá por:

I. Afectado o interesado: persona física titular de los datos que sean objeto de tratamiento a que se refiere la fracción XVI de esta norma;

II. Cancelación: procedimiento por el cual el responsable del fichero, una vez terminado el uso declarado de los datos, de oficio o a solicitud del interesado, se inhabilita el acceso a los registros que los contienen, ya sea por su supresión total o parcial, o por la depuración del archivo que los soporta.

III. Cesión o comunicación de datos: toda revelación de datos realizada a una persona física o moral distinta del interesado;

IV. Comisión: la Comisión Estatal de Garantía de Acceso a la Información Pública del Estado de San Luis Potosí;

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

VI. Dato disociado: aquel que no permite la identificación de un afectado o interesado;

VII. Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas e identificables;

VIII. Datos sensibles: cualquier información que se encuentre íntimamente relacionada con el honor, la reputación y la dignidad de las personas, y sea susceptible de causar una seria afectación en los mismos;

IX. Encargado del tratamiento: la persona física o moral, autoridad pública o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

X. Fichero: todo conjunto organizado de datos, como archivos, registros, bases y bancos de datos, etc., que contengan datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso;

XI. Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación;

XII. Ley: la Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí;

XIII. Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable;

XIV. Responsable del fichero o tratamiento: persona física o moral, autoridad pública o cualquier otro organismo que decida sobre la finalidad, contenido y uso del tratamiento de datos;

XV. SEDA: el Sistema Estatal de Documentación y Archivo,

XVI. Tratamiento de datos: el conjunto de operaciones y procedimientos técnicos de carácter automatizado o no, que permitan grabar, conservar, elaborar, organizar, modificar, bloquear, cancelar, o ceder los datos previamente fueron recabados del afectado o interesado; y

XVII. Usuario: el servidor público facultado por una norma legal o reglamentaria o expresamente autorizado por el responsable del fichero, que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de modificar o agregar su contenido.

XVIII. Derecho de acceso: es la prerrogativa de toda persona para identificar y conocer la información personal bajo resguardo de un ente obligado, su forma de recolección, su tratamiento y toda información relativa al uso y destino de sus datos personales.

XIX. Derecho de rectificación: es la prerrogativa de toda persona para modificar la información errónea, inexacta o sin actualizar, relativa a sus datos personales, sujeta a las disposiciones legales y procedimientos específicos.

XX. Derecho de oposición: es la prerrogativa de toda persona a negarse al tratamiento de su información personal, sin menoscabo de su recolección para los fines que le sean comunicados.

XXI. Derecho de cancelación: es la prerrogativa de toda persona para solicitar la supresión de sus datos personales de los ficheros o bases de datos que los contengan, sin menoscabo de la conservación de información de carácter histórico, estadístico o científico, previo procedimiento de disociación.

CAPÍTULO II

Principios de la Protección de Datos

Sección Primera

De la calidad de los datos

QUINTA. Ninguna persona está obligada a dar información que pudiera propiciar expresión de discriminación e intolerancia sobre su persona, honor, reputación y dignidad.

SEXTA. Los datos de carácter personal sólo podrán ser recabados para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del fichero o tratamiento para las que se hayan obtenido, y no se podrá requerir a las personas información que exceda los fines para los cuales se solicita.

SÉPTIMA. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recabados. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

OCTAVA. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recabados directamente del afectado, se considerarán exactos los facilitados por éste.

NOVENA. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, siempre y cuando posean los documentos que justifiquen la actualización, dando aviso de ello al interesado, sin perjuicio de las facultades que a los afectados se reconocen en el Capítulo III de estas Normas.

DÉCIMA. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Una vez cancelados, sólo podrán ser conservados en forma tal que no permita la identificación del interesado.

DÉCIMO PRIMERA. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

DÉCIMO SEGUNDA. Se prohíbe recabar datos por medios fraudulentos, desleales o ilícitos.

DÉCIMO TERCERA. Los afectados o interesados a quienes se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de:

- I. La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de recabar éstos y de los destinatarios de la información;
- II. El carácter obligatorio o facultativo de entregar los datos que le sean requeridos;
- III. Las consecuencias de proporcionar los datos o de la negativa a suministrarlos;
- IV. La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, informando el procedimiento a seguir; y

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

DÉCIMO CUARTA. Cuando se utilicen cuestionarios u otros impresos para recabar datos de carácter personal, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere la norma anterior, el tratamiento a que serán sometidos y la finalidad del sistema al que serán incorporados.

Las dependencias y entidades al solicitar los datos personales deberán mostrar la siguiente leyenda en todo formato mediante el cual se recaben datos personales:

“Los datos personales recabados serán protegidos y serán incorporados y tratados en el sistema de datos personales (**indicar el nombre del sistema de datos personales**), con fundamento en (**indicar el fundamento legal que faculta a la dependencia o entidad para recabar los datos personales en el sistema de datos personales**) y cuya finalidad es (**describir la finalidad del sistema de datos personales**), el cual fue registrado en el listado de sistemas de datos personales ante la Comisión Estatal de Garantía de Acceso a la Información Pública (www.cegaip.org.mx), y podrán ser transmitidos a (**indicar las personas u organismos a los que podrán transmitirse los datos personales contenidos en el sistema de datos personales**), con la finalidad de (**describir la finalidad de la transmisión**), además de otras transmisiones previstas en la Ley. El responsable del sistema de datos personales es (**indicar el nombre de la unidad administrativa responsable del sistema de datos personales**), y la dirección donde el interesado podrá ejercer los derechos de acceso y corrección ante la misma es (**indicar la dirección de la unidad de información pública de la dependencia o entidad que posee el sistema de datos personales**). Lo anterior se informa en cumplimiento de la norma Décima Cuarta de los Normas para el Tratamiento y Protección de Datos Personales, publicados en el Periódico Oficial del Estado (**anotar la fecha de publicación en el Periódico Oficial del Estado de las presentes Normas**).

DÉCIMO QUINTA. Cuando los datos de carácter personal no hayan sido recabados del afectado o interesado, éste deberá ser informado en forma expresa, precisa e inequívoca, por el responsable del fichero o su representante dentro del término de diez días hábiles siguientes al momento del registro de los datos, para que exprese su consentimiento respecto de su recolección y tratamiento.

La falta de comunicación a que se refiere el párrafo anterior, traerá como consecuencia la cancelación inmediata de los datos recabados.

DÉCIMO SEXTA. No aplicará lo dispuesto en la norma anterior cuando:

I. El tratamiento tenga fines históricos, estadísticos o científicos;

II. Los datos procedan de fuentes de acceso público

III. La información al interesado resulte imposible o exija un esfuerzo desproporcionado, a juicio de la CEGAIP en consideración al interés público.

DÉCIMO SÉPTIMA. A efecto de cumplir con el principio de calidad a que se refiere esta sección, se considera que la recolección de datos personales es:

a) Exacta: Cuando los datos personales se mantienen actualizados y relacionados con el hecho real que describen, de manera tal que no altere la veracidad de la información que traiga como consecuencia que el Titular de los datos se vea afectado por dicha situación;

b) Adecuada: propósito de la recogida de datos se deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.

c) Pertinente: En congruencia con el ámbito de atribuciones de la autoridad y con la finalidad para los que fueron recogidos con el objeto de ser tratados posteriormente, y

d) No excesiva: Cuando la información solicitada al Titular de los datos no exceda de la estrictamente necesaria para cumplir con los fines para los cuales se hubieran recabado.

Sección Segunda **Del consentimiento, el tratamiento y la cesión**

DÉCIMO OCTAVA. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo los casos expresamente contemplados en el artículo 53 de la Ley.

El tratamiento de los datos de los menores e incapaces, solo podrá realizarse con el expreso consentimiento de los padres o tutores.

Queda expresamente prohibido recabar de los menores e incapaces datos que permitan obtener información sobre los demás miembros de la familia, sin el consentimiento de los titulares de dichos datos. Se exceptúan de lo anterior los datos relativos a la identidad y dirección de los padres o tutores para el efecto de recabar la autorización a que se refiere el párrafo anterior.

DÉCIMO NOVENA. Para el tratamiento de los datos de menores e incapaces a que se refiere la norma anterior, el responsable del fichero o tratamiento deberá acreditar, en todo momento, la comprobación de la edad del menor o la condición del incapaz así como la autenticidad del consentimiento prestado por quien legítimamente pudiera hacerlo.

VIGÉSIMA. En cuanto a los datos personales de un individuo que haya fallecido, podrán tener acceso solamente sus familiares en línea recta sin limitación de grado o colaterales hasta el tercer grado, debiendo acreditar dicha circunstancia con los documentos idóneos correspondientes.

VIGÉSIMO PRIMERA. Además de lo dispuesto por la disposición quinta de estas Normas, nadie podrá ser obligado a declarar sobre su ideología, afiliación sindical, religión, creencias o vida sexual.

VIGÉSIMO SEGUNDA. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento, se advertirá al afectado o interesado de su derecho a no prestarlo.

VIGÉSIMO TERCERA. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual o preferencia sexual, sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado o interesado consienta expresamente.

VIGÉSIMO CUARTA. Los ficheros creados por los órganos de seguridad pública que contengan datos de carácter personal que, por haberse recabado para fines administrativos, deban ser objeto de registro permanente, estarán sujetos a la Ley y a estas disposiciones.

VIGÉSIMO QUINTA. El recabado y tratamiento para fines policiales de datos de carácter personal por los órganos de seguridad pública sin consentimiento de las personas afectadas, están limitados a

aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para inhibir infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

VIGÉSIMO SEXTA. El recabado y tratamiento por parte de los órganos de seguridad pública de los datos a que hacen referencia las disposiciones vigésimo primera, vigésimo segunda y vigésimo tercera de las presentes Normas, 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 en su caso por los interesados que correspondan a los órganos jurisdiccionales.

VIGÉSIMO SÉPTIMA. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos almacenados 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.

VIGÉSIMO OCTAVA. El tratamiento de los datos personales sólo se realizará con el consentimiento del interesado, el que se expresará por escrito en el momento en que se recaben dichos datos, dando previo cumplimiento a las disposiciones Décimo Tercera y Décimo Cuarta de estas Normas.

En el supuesto previsto en la disposición Décimo Quinta, se otorgará al interesado un plazo de diez días hábiles para manifestar su negativa al tratamiento, apercibiéndole que de no manifestar oposición alguna, se entenderá consentido el tratamiento de sus datos personales.

El responsable quedará impedido de proceder al tratamiento de los datos personales respectivos, sino consta fehacientemente la recepción de la comunicación a que se refiere el párrafo anterior por el afectado.

El responsable deberá facilitar al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En todo caso el medio deberá darse a conocer al interesado desde la comunicación a que se refiere el párrafo segundo de esta misma norma.

Si el interesado negare su consentimiento para el tratamiento de sus datos personales, en términos de éste precepto, dicho consentimiento no podrá solicitarse nuevamente respecto del mismo tratamiento en el plazo de un año contado a partir de la fecha de la anterior solicitud.

Sin perjuicio de lo establecido en la presente norma, el interesado podrá en todo momento ejercer su derecho de oposición al tratamiento de sus datos de carácter personal.

VIGÉSIMO NOVENA. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las fuentes legítimas del cedente y del cesionario con el previo consentimiento del interesado, salvo los casos a que se refiere el artículo 53 de la Ley.

TRIGÉSIMA. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

TRIGÉSIMO PRIMERA. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

TRIGÉSIMO SEGUNDA. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la Ley.

TRIGÉSIMO TERCERA. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en las disposiciones vigésimo tercera a vigésimo sexta de estas Normas.

TRIGÉSIMO CUARTA. No se considerará comunicación de datos el acceso de un tercero a los datos, cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que conste por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciendo expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no lo aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán las medidas de seguridad que procedan, conforme a lo que se establece en el Capítulo IV de estas Normas.

TRIGÉSIMO QUINTA. Una vez cumplida la prestación contractual a la que se refiere la norma anterior, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

TRIGÉSIMO SEXTA. En el caso de que el tercero encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TRIGÉSIMO SÉPTIMA. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación partidista, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual o preferencia sexual.

CAPÍTULO III

Derechos de Acceso, Rectificación, Cancelación y Oposición

Sección Primera

Disposiciones generales

TRIGÉSIMO OCTAVA. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y sólo podrán ser ejercidos por el afectado, acreditando su identidad, o por representante legal expresamente facultado para el ejercicio de estos derechos.

Tratándose de menores e incapaces el ejercicio de los derechos enunciados se hará por conducto de los padres o tutores, debiendo acreditarse tal condición.

Las solicitudes de acceso, rectificación, cancelación y oposición formuladas por terceros que no acrediten la representación legal en términos de este precepto, serán desechadas, sin perjuicio de que

el afectado presente una nueva solicitud por sí o por persona que acredite debidamente su representación legal.

TRIGÉSIMO NOVENA. Se considerarán excepciones a los derechos de acceso, rectificación y cancelación, siempre y cuando se fundamente y motive la prueba de interés público, en los siguientes casos:

I. Los responsables de los ficheros que contengan datos a los que se refieren las disposiciones vigésimo cuarta a vigésimo sexta de estas Normas podrán negar el acceso, rectificación, cancelación u oposición en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la vida y la salud de las personas, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, y

II. Los responsables de los ficheros de las autoridades fiscales estatales y municipales podrán negar el acceso, rectificación o cancelación de datos personales cuando el ejercicio de esos derechos obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado o interesado esté siendo sujeto de las facultades de comprobación de las citadas autoridades.

CUADRAGÉSIMA. Los derechos de acceso, rectificación, cancelación y oposición son independientes entre sí, por lo que no deberá exigirse el ejercicio de uno, como requisito previo al ejercicio de otro.

CUADRAGÉSIMO PRIMERA. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición será gratuito y se realizará a través de medios sencillos que no impliquen para el afectado erogaciones mayores o injustificadas, ni para el ente obligado la oportunidad de ingresos adicionales a los propios de su actividad.

CUADRAGÉSIMO SEGUNDA. Las solicitudes de acceso, rectificación, cancelación y oposición se presentarán por escrito dirigido a la Unidad de Información Pública correspondiente, en el que se indicará:

- I. Nombre del Solicitante y de su representante legal, en su caso;
- II. Domicilio para recibir notificaciones;
- III. Objeto de la solicitud;
- IV. El nombre del sistema, fichero o base de datos personales al que desea acceder, si lo conociere.

A la solicitud deberán adjuntarse los documentos que acrediten tanto la identidad del afectado, como el objeto de la solicitud, en su caso.

Cuando se omita alguno de los requisitos mencionados o no se anexe la documentación que se precisa en el párrafo que antecede, el responsable deberá prevenir al afectado para que los subsane en un plazo no mayor de cinco días hábiles, apercibiéndole que de no hacerlo, la solicitud se le tendrá por no presentada, lo que no será obstáculo para la presentación de una nueva solicitud respecto del mismo objeto.

CUADRAGÉSIMO TERCERA. La Unidad de Información Pública deberá, sin excepción alguna responder las solicitudes en un plazo de diez días hábiles, con independencia de que figuren o no datos personales en sus ficheros y entregarlos.

La resolución deberá ajustarse a lo dispuesto para cada caso en las distintas secciones de éste capítulo.

El responsable del fichero o tratamiento deberá informar a la CEGAIP acorde con lo dispuesto a la Ley, sobre las negativas a las solicitudes que presenten los afectados.

CUADRAGÉSIMO CUARTA. Contra las negativas recaídas a las solicitudes de acceso, rectificación, cancelación y oposición, los afectados podrán ocurrir en queja ante la CEGAIP, de conformidad con las disposiciones relativas de la Ley.

Sección Segunda Derecho de acceso

CUADRAGÉSIMO QUINTA. El Derecho de Acceso es el derecho del afectado a obtener información sobre sus propios datos de carácter personal que están siendo objeto de tratamiento, la finalidad de éste y la información disponible sobre el origen de éstos datos así como las comunicaciones realizadas o previstas respecto de los mismos.

CUADRAGÉSIMO SEXTA. El Derecho de Acceso faculta al afectado a obtener del responsable del tratamiento la información relativa a datos concretos, datos incluidos en un determinado fichero o a la totalidad de sus datos sometidos a tratamiento.

CUADRAGÉSIMO SÉPTIMA. En el escrito por el que se ejerza el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consultas del fichero:

I. Visualización en pantalla;

II. Oficio, copia o fotocopia remitida por correo ordinario o certificado con acuse de recibo;

III. Fax;

IV. Correo electrónico, y

V. Cualquier otro sistema que resulte adecuado a la naturaleza y estado de los ficheros y la información en éstos contenida.

CUADRAGÉSIMO OCTAVA. En el caso que el ente obligado no cuente con alguno o algunos de los sistemas de consulta que se establecen en la norma anterior, lo comunicará al afectado, ofreciéndole aquel o aquellos sistemas con los que efectivamente cuente.

CUADRAGÉSIMO NOVENA. El responsable del fichero o tratamiento podrá negar el acceso a la información siempre que exista una causa debidamente fundada en la ley, éstas normas o en las demás disposiciones legales y administrativas aplicables, haciéndolo del conocimiento de la CEGAIP.

Sección Tercera Derechos de Rectificación y cancelación

QUINCUAGÉSIMA. En virtud del ejercicio del derecho de rectificación, el afectado podrá solicitar la modificación de los datos que resulten ser inexactos o incompletos.

QUINCUAGÉSIMO PRIMERA. A través del ejercicio del derecho de cancelación se suprimirán los datos que resulten ser inadecuados o excesivos, sin perjuicio del bloqueo que proceda conforme a éstas normas.

QUINCUAGÉSIMO SEGUNDA. Si los datos rectificadas o cancelados hubieran sido cedidos previamente, el responsable deberá comunicar la rectificación o cancelación efectuada al cesionario dentro del plazo de diez días contados a partir de que se emita la resolución correspondiente. A su vez, el cesionario contará con idéntico plazo, a partir de recibida la comunicación, para rectificar o cancelar los datos en los mismos términos, lo que necesariamente deberá también ser notificado al afectado en el mismo plazo.

QUINCUAGÉSIMO TERCERA. La cancelación no procederá cuando los datos personales deban ser conservados durante los plazos previstos en las disposiciones legales aplicables, o, en su caso, en las relaciones contractuales entre la entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

Sección Cuarta Derecho de oposición

QUINCUAGÉSIMO CUARTA. El ejercicio del derecho de oposición del afectado impide que se lleve a cabo el tratamiento de sus datos de carácter personal, o bien produce el cese de dicho tratamiento.

QUINCUAGÉSIMO QUINTA. Los interesados tienen el legítimo derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que los afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad como su rendimiento laboral, fiabilidad o conducta.

La valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Se exceptúan de lo establecido en el primer párrafo de esta misma norma las decisiones que se adopten por encontrarse autorizadas en una disposición legal vigente o en cumplimiento de un acuerdo de voluntades, y siempre que se haya informado al afectado previamente de que dichas decisiones podrían ser adoptadas.

CAPÍTULO IV Seguridad en la Protección de Datos Personales

QUINCUAGÉSIMO SEXTA. Las entidades, servidores públicos y demás entes obligados que posean datos personales, deberán tomar las medidas técnicas para proteger los archivos y sistemas de archivo que resguarden datos personales contra los riesgos naturales, la pérdida por siniestro o accidentes y contra el riesgo de que se acceda a ellos sin autorización, se utilicen de manera encubierta o se contaminen por virus informático.

QUINCUAGÉSIMO SÉPTIMA. Las entidades, servidores públicos y demás entes obligados deberán informar mensualmente a la CEGAIP acerca de la actualización de los sistemas de archivo de los datos personales en su poder.

QUINCUAGÉSIMO OCTAVA. Se establecen tres niveles de seguridad para la protección de los datos personales, cuyas pautas aplican de igual manera a los archivos no informatizados, que, conforme a la naturaleza de la información tratada, son los siguientes:

I. Nivel Básico: Aplican a los ficheros que contengan datos personales;

II. Nivel Medio: Aplican a los ficheros de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como a los pertenecientes a entidades públicas y demás entes obligados que cumplan una función pública que deban guardar secreto de la información personal por expresa disposición legal, y

III. Nivel Crítico: Aplican a los ficheros que contengan datos personales, definidos como datos sensibles.

QUINCUAGÉSIMO NOVENA. Los entes obligados deberán contar con un Expediente de Seguridad de Datos Personales en el que se especifiquen los procedimientos y las medidas a adoptar para garantizar la protección de los datos personales específicas para cada uno de los niveles de seguridad a que se refiere la norma anterior. El Expediente de Seguridad de Datos Personales deberá mantenerse en todo momento actualizado y ser revisado cuando se produzcan cambios en el sistema de información.

SEXAGÉSIMA. El Expediente a que se refiere la Norma Quincuagésima Novena de esta disposición, deberá adoptar las siguientes medidas de seguridad para el Nivel Básico:

I. Funciones y obligaciones del personal;

II. Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan;

III. Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento, deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes;

IV. Registros de incidentes de seguridad, que incluyan el procedimiento de notificación, gestión y respuesta ante los incidentes de seguridad;

V. Procedimientos para efectuar las copias de respaldo y de recuperación de datos;

VI. Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso;

VII. Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información. La relación entre el usuario autorizado y el o los sistemas de información a los que puede acceder debe mantenerse actualizada. En el caso en que el mecanismo de autenticación utilice contraseña, la misma será asignada por el responsable de seguridad de acuerdo a un procedimiento que garantice su confidencialidad. Este procedimiento deberá prever el cambio periódico de la contraseña, lapso máximo de vigencia, las que deberán estar almacenadas en forma ininteligible;

VIII. Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados;

IX. Adopción de medidas de prevención a efectos de impedir amenazas de software malicioso, tales como virus, troyanos, etc., que puedan afectar archivos con datos de carácter personal, entre las que deben considerarse, cuando menos:

- a) instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente.
- b) Verificar, antes de su uso, la inexistencia de virus en archivos recibidos a través de la web, correo electrónico y otros cuyos orígenes sean inciertos, y

X. Procedimiento que garantice una adecuada Gestión de los Soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringidos, inventarios, autorización para su salida fuera del local en que están ubicados, destrucción de la información en desuso, etc.).

Cuando los ficheros contengan una serie de datos personales con los cuales, a través de un determinado tratamiento, se permita establecer el perfil de personalidad o determinadas conductas de la persona, se deberán garantizar las medidas de seguridad del presente nivel más las establecidas en las fracciones II, III, IV y V de la norma siguiente.

SEXAGÉSIMO PRIMERA. El expediente a que se refiere la Norma Quincuagésimo Novena de esta disposición, deberá disponer que, además de las medidas de seguridad del Nivel Básico, los ficheros correspondientes al Nivel Medio deberán adoptar las siguientes:

- I. Identificar al Responsable de Seguridad;
- II. La realización de auditorías internas o externas que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales. Los informes de auditoría pertinentes, serán presentados al Responsable del Archivo a efectos de que se adopten las medidas correctivas que correspondan. La CEGAIP, en las inspecciones que realice, deberá considerar obligatoriamente, con carácter no vinculante, los resultados de las auditorías referidas, siempre que las mismas hayan sido realizadas dentro de un período máximo de un año;
- III. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información;
- IV. Se establecerá un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal;
- V. Gestión de Soportes e información contenida en ellos, para lo cual:
 - a) Se dispondrá de un registro de entradas y salidas de los soportes informáticos de manera de identificar, día y hora de entrada y salida del soporte, receptor, emisor, forma de envío, etc.
 - b) Se adoptarán las medidas necesarias para impedir cualquier recuperación de la información con posterioridad a que un soporte vaya a ser desechado o reutilizado, o que la información deba ser destruida, por la causa que correspondiere. Asimismo se deberán adoptar similares medidas cuando los soportes, o la información vaya a salir fuera de los locales de soporte local en que se encuentren ubicados, ya sea a través copias de respaldo o de una red de transmisión de datos.

c) Se deberá disponer de un procedimiento de recuperación de la información de respaldo y de tratamiento de la misma en caso de contingencias que pongan no operativo, los equipos de procesamiento habituales;

VI. Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar a la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado, y

VII. Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa no se realizarán con datos o archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados.

SEXAGÉSIMO SEGUNDA. El Expediente a que se refiere la Norma Quincuagésimo Novena de esta disposición, deberá disponer que, además de las medidas de seguridad de los Niveles Básico y Medio, los ficheros correspondientes al Nivel Crítico, deberán adoptar las siguientes:

I. Cuando se distribuyan soportes que contengan archivos con datos de carácter personal, incluidas las copias de respaldo, se deberán cifrar dichos datos o utilizar cualquier otro mecanismo, a fin de garantizar que no puedan ser leídos o manipulados durante su transporte;

II. Se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, la fecha y la hora en que lo hizo, tipo de acceso y si fue autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo. Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como mínimo por el término de tres años;

III. Además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo los equipos de procesamiento habituales, y

IV. Los datos de carácter personal que se transmitan a través de redes de comunicación que salgan fuera de la red del ente obligado, deberán ser cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas.

Quedan exceptuados de aplicar las medidas de seguridad de Nivel Crítico, los ficheros que deban efectuar el tratamiento de datos sensibles para fines administrativos o por obligación legal. No obstante, ello no excluye que igualmente deban contar con aquellas medidas de resguardo que sean necesarias y adecuadas al tipo de dato.

CAPÍTULO V

Creación, Modificación y Supresión de Ficheros

SEXAGÉSIMO TERCERA. Las unidades de información pública responsables de atender las solicitudes de información, en coordinación con el SEDA, establecerán las medidas técnicas necesarias para sistematizar y archivar con fines lícitos y legítimos la información que contenga datos personales. Para tal efecto, desarrollarán el Registro de Protección de Datos Personales, bajo la coordinación de la CEGAIP a través del SEDA, en el que se llevará un registro de los ficheros que contengan datos

personales, en el que se especifique el tipo de tratamiento de datos personales, sus finalidades, la identidad del responsable del tratamiento y el nivel de seguridad bajo el que se encuentre. El registro será de consulta pública y gratuita.

SEXAGÉSIMO CUARTA. La creación, modificación o supresión de los ficheros de las entidades públicas, sólo podrán hacerse por medio de disposición general publicada en el Periódico Oficial del Estado.

SEXAGÉSIMO QUINTA. Las disposiciones de creación o modificación de ficheros deberán indicar:

- I. La finalidad del fichero y los usos previstos para el mismo;
- II. Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;
- III. El procedimiento empleado para recabar los datos de carácter personal;
- IV. La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo;
- V. Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean;
- VI. Los órganos de las entidades públicas responsables del fichero;
- VII. Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición, y
- VIII. Las medidas de seguridad con indicación del nivel básico, medio o crítico exigible.

SEXAGÉSIMO SEXTA. En las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

SEXAGÉSIMO SÉPTIMA. El SEDA y las unidades de información pública dispondrán de los medios necesarios para que las personas interesadas estén en condiciones de ejercer la acción de protección de datos personales, para asegurarse que:

- I. Los datos personales en posesión de la autoridad siguen siendo necesarios para cumplir los fines para los que fueron requeridos;
- II. Los datos personales no se utilicen o pongan a disposición del público o de terceros sin el previo consentimiento del interesado o su representante legal, con propósitos distintos e incompatibles con los fines originalmente señalados, y
- III. Que los datos personales no hayan estado a disposición de la autoridad por un periodo superior al necesario.

SEXAGÉSIMO OCTAVA. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la Ley y estas Normas y, en particular, cuando tales datos resulten inexactos o incompletos.

SEXAGÉSIMO NOVENA. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las autoridades competentes para la atención de posibles responsabilidades derivadas de su tratamiento, durante el plazo de prescripción de éstas. Cumplido el plazo deberá procederse a la supresión de los datos.

CAPÍTULO VI

Promoción del derecho de protección de datos personales

SEPTUAGÉSIMA. La CEGAIP, con el apoyo de los servidores públicos y los entes obligados, promoverá que en los planes y programas de la educación que imparten las instituciones públicas y privadas en el Estado, en todos sus niveles y modalidades, se incluyan contenidos relacionados con el ejercicio del derecho de acceso, rectificación y cancelación de datos personales.

SEPTUAGÉSIMO PRIMERA. La CEGAIP con el apoyo de los entes obligados, promoverá la realización de actividades encaminadas a fortalecer la cultura de la protección de datos personales entre los servidores públicos.

SEPTUAGÉSIMO SEGUNDA. La CEGAIP, con el apoyo de los entes obligados, realizará campañas públicas de difusión para favorecer entre la población el conocimiento de sus derechos de protección de datos personales, entre los que se destaque especialmente:

- I. Los derechos de acceso, rectificación y cancelación de datos personales;
- II. El derecho de las personas a quienes se soliciten datos personales a contar con información sobre los fines para los que se le solicitan en los términos del artículo 13 de estas Normas;
- III. El derecho de las personas a otorgar o negar su consentimiento para el tratamiento de los datos personales, y
- IV. El reconocimiento de todos sus derechos, los procedimientos y formularios para ejercerlos y las instancias a las que puede acudir para hacerlos valer.

CAPÍTULO VII

Del Procedimiento administrativo de Verificación

SEPTUAGÉSIMO TERCERA. La CEGAIP verificará, en cualquier tiempo, el cumplimiento de las obligaciones que en materia de datos personales establecen la Ley y las presentes Normas a cargo de los entes obligados, sujetándose en todo caso al siguiente procedimiento:

- I. La GEGAIP solicitará por oficio al ente obligado la documentación que estime necesaria para verificar el debido tratamiento y protección de datos personales;
- II. Dentro de los quince días hábiles siguientes a la fecha de notificación de la solicitud de documentación, la entidad pública remitirá a la CEGAIP, en sobre cerrado, los documentos solicitados. El sobre deberá contener en la parte exterior una leyenda que indique el contenido del mismo;
- III. Cuando del análisis efectuado a la documentación que le fuese proporcionada en términos de la fracción precedente, la CEGAIP no encontrase irregularidad alguna, lo comunicará por oficio a la entidad pública y dará por concluida la revisión;

IV. Si del análisis que la CEGAIP practique a la documentación proporcionada en términos de la fracción II de esta norma, encuentra que no se satisfacen las disposiciones aplicables en la materia, notificará tal circunstancia al ente obligado en forma fundada y motivada, emplazándola para que en un plazo no mayor de quince días hábiles siguientes a la fecha de notificación, haga las manifestaciones y aporte, en su caso, las pruebas que estime conducentes;

V. Transcurrido el plazo a que se refiere la fracción anterior, con independencia de que el ente obligado haya hecho uso o no de su derecho a realizar las manifestaciones o a presentar las pruebas que le correspondan, la CEGAIP emitirá la resolución que proceda, notificándola al ente obligado dentro de los cinco días hábiles siguientes;

VI. Siempre que la CEGAIP determine que existe incumplimiento a la Ley y a estas Normas, dictará las medidas que estime pertinentes a efecto de corregir las irregularidades de que se trate, y

VII. El ente obligado contará con un plazo de diez días hábiles para cumplimentar la resolución que la CEGAIP dicte en términos de la fracción que antecede.

La CEGAIP no podrá publicar o dar a conocer información relacionada con las verificaciones que se encuentre efectuando, mientras estas se encuentren en trámite.

SEPTUAGÉSIMO CUARTA. Cuando con motivo de una verificación, la CEGAIP conozca de infracciones que se ubiquen en los supuestos previstos en el artículo 109 de la Ley, iniciará contra el presunto infractor el procedimiento sancionador en los términos del diverso numeral 116 de la propia Ley.

SEPTUAGÉSIMO QUINTA. La verificación a que se refiere el presente Capítulo, es distinta y se ejercerá sin perjuicio de las facultades que a la CEGAIP corresponden en la tramitación de las Quejas que, en su caso, presenten los particulares en materia de protección de datos personales.

TRANSITORIOS

PRIMERO. Las presentes Normas entrarán en vigor al día siguiente de su publicación en el Periódico Oficial del Estado.

SEGUNDO. Se dejan sin efectos las medidas de carácter administrativo implementadas por los Entes Obligados que se opongan a esta Normas.

TERCERO. Los entes obligados, contarán con un plazo de seis meses a partir de la publicación de las presentes Normas, para elaborar los Expedientes de Seguridad a que se refiere la disposición Quincuagésimo Novena de estas Normas, haciéndolo del conocimiento de la CEGAIP.

CUARTO. El Sistema Estatal de Documentación y Archivo, en coordinación con las Unidades de Información Pública, integrarán el Registro Estatal de Protección de Datos en un plazo de dieciocho meses a partir de la publicación de las presentes Normas.