Publicada en el Periódico Oficial "Gaceta del Gobierno" el 30 de mayo de 2017.
Sin reforma.

ERUVIEL ÁVILA VILLEGAS, Gobernador Constitucional del Estado Libre y Soberano de México, a sus habitantes sabed:

Que la Legislatura del Estado, ha tenido a bien aprobar lo siguiente:

DECRETO NÚMERO 209

LA H. "LIX" LEGISLATURA DEL ESTADO DE MÉXICO
DECRETA:

ARTÍCULO ÚNICO. Se expide la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, para quedar como sigue:

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE MÉXICO Y MUNICIPIOS

TÍTULO PRIMERO
DE LAS DISPOSICIONES GENERALES

CAPÍTULO PRIMERO
DEL OBJETO Y ÁMBITO DE APLICACIÓN DE LA LEY

Del objeto de la Ley
Artículo 1. La presente Ley es de orden público, interés social y observancia obligatoria en el Estado de México y sus Municipios. Es reglamentaria de las disposiciones en materia de protección de datos personales previstas en la Constitución Política del Estado Libre y Soberano de México.

Tiene por objeto establecer las bases, principios y procedimientos para tutelar y garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los sujetos obligados.

De las finalidades de la Ley
Artículo 2. Son finalidades de la presente Ley:

I. Proveer lo necesario para que toda persona pueda ejercer su derecho fundamental a la protección de datos personales.

II. Garantizar la observancia de los principios de protección de datos personales en posesión de los sujetos obligados.

III. Determinar procedimientos sencillos y expeditos para el acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

IV. Proteger los datos personales en posesión de los sujetos obligados del Estado de México y municipios a los que se refiere esta Ley, con la finalidad de regular su debido tratamiento.

V. Promover la adopción de medidas de seguridad que garanticen, la integridad, disponibilidad y confidencialidad de los datos personales en posesión de los sujetos obligados, estableciendo los mecanismos para asegurar su cumplimiento.

VI. Contribuir a la mejora de procedimientos y mecanismos que permitan la protección de los datos personales en posesión de los sujetos obligados.

VII. Promover, fomentar y difundir una cultura de protección de datos personales en el Estado de México y sus Municipios.

VIII. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio para aquellas conductas que contravengan las disposiciones previstas en esta Ley.

IX. Establecer la competencia y funcionamiento del Instituto de Transparencia, Acceso a la Información Pública y Protección de Personales del Estado de México y Municipios en materia de protección de datos personales.

X. Regular los medios de impugnación en la materia y los procedimientos para su interposición ante el Instituto de Transparencia, Acceso a la Información Pública y Protección de Personales del Estado de México y Municipios.

De los Sujetos Obligados
Artículo 3. Son sujetos obligados por esta Ley:

I. El Poder Ejecutivo.

II. El Poder Legislativo.

III. El Poder Judicial.

IV. Los Ayuntamientos,

V. Los Órganos y Organismos Constitucionales Autónomos.

VI. Los Tribunales Administrativos.

VII. Los Partidos Políticos.

VIII. Los Fideicomisos y Fondos Públicos.

Los sindicatos, las candidatas o los candidatos independientes y cualquier otra persona física o jurídica colectiva que reciba y ejerza recursos públicos o realice actos de autoridad serán responsables de los datos personales de conformidad con las disposiciones legales aplicables para la protección de datos personales en posesión de los particulares.

En los demás supuestos, las personas físicas y jurídicas colectivas se sujetarán a lo previsto en las disposiciones legales aplicables.

Glosario
Artículo 4. Para los efectos de esta Ley se entenderá por:

I. Administrador: a la servidora o el servidor público o persona física facultada y nombrada por el Responsable para llevar a cabo tratamiento de datos personales y que tiene bajo su responsabilidad los sistemas y bases de datos personales.

II. Anonimización: al tratamiento que permite evitar la identificación de la o el titular a través de sus datos personales.

III. Archivo: al conjunto de documentos en cualquier soporte, producidos o recibidos por los sujetos

obligados en el ejercicio de sus atribuciones o desarrollo de sus actividades.

IV. Áreas o Unidades Administrativas: a las instancias que pertenecen los sujetos obligados que cuenten o puedan contar, dar tratamiento y ser responsables o encargados, usuarias o usuarios de los sistemas y bases de datos personales previstos en las disposiciones legales aplicables.

V. Aviso de Privacidad: al documento físico, electrónico o en cualquier formato generado por el responsable que es puesto a disposición del Titular con el objeto de informarle los propósitos del tratamiento al que serán sometidos sus datos personales.

VI. Base de Datos: al conjunto de archivos, registros, ficheros, condicionados a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento, organización y acceso.

VII. Bloqueo: a la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual, transcurrido este se procederá a su cancelación en los sistemas y bases de datos que corresponda.

VIII. Cómputo en la nube: al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

IX. Consejo Nacional: al Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

X. Consentimiento: a la manifestación de la voluntad libre, específica, informada e inequívoca de la o el titular de los datos personales para aceptar el tratamiento de su información.

XI. Datos personales: a la información concerniente a una persona física o jurídica colectiva identificada o identificable, establecida en cualquier formato o modalidad, y que esté almacenada en los sistemas y bases de datos, se considerará que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier documento informativo físico o electrónico.

XII. Datos personales sensibles: a las referentes de la esfera de su titular cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud física o mental, presente o futura, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

XIII. Derechos ARCO: a los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.

XIV. Destinatario: a la persona física o jurídica colectiva pública o privada a quien el responsable transfiere datos personales.

XV. Días: a los días hábiles.

XVI. Disociación: al procedimiento por el que los datos personales no pueden asociarse a la o el titular, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo.

XVII. Documentos: a los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, convenios, contratos, instructivos, notas, memorándums, estadísticas, o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en formato escrito, sonoro, visual, electrónico, informático, holográfico o de tecnología de información existente.

XVIII. Documento de seguridad: al instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de la información contenida en los sistemas y bases de datos personales.

XIX. Encargado: a la persona física o jurídica colectiva, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

XX. Evaluación de impacto en la protección de datos personales: al documento por el que los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas, bases o plataformas informáticas, aplicaciones electrónicas, cualquier otra tecnología o procedimiento que implique el tratamiento intensivo o relevante de datos personales, valoran y establecen con parámetros cualitativos y/o cuantitativos los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios y deberes aplicables al tratamiento y derechos de las y los titulares, así como los deberes de los responsables y encargados, previstos en esta Ley y demás disposiciones legales aplicables.

XXI. Fuentes de acceso público: a los sistemas y bases de datos que por disposición de Ley puedan ser consultadas públicamente, cuando no exista impedimento por una norma limitativa y sin más exigencia en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita.

XXII. Instituto: al Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios.

XXIII. Instituto Nacional: al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

XXIV. Ley: a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.

XXV. Ley de Transparencia: a la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

XXVI. Ley General: a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

XXVII. Lineamientos: a las disposiciones emitidas por el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, que contienen las políticas, criterios y procedimientos, para garantizar a las y los titulares la protección de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transferencia ilícita.

XXVIII. Limitación del tratamiento: al marcado de datos de carácter personal conservados con el fin de limitar su uso en el futuro.

XXIX. Medidas compensatorias: a los mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.

XXX. Medidas de seguridad: a las acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

XXXI. Medidas de seguridad administrativas: a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, y capacitación del personal, en materia de protección de datos personales.

XXXII. Medidas de seguridad físicas: a las acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se considerarán las actividades siguientes:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización.

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad e integridad.

XXXIII. Medidas de seguridad técnicas: a las acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se considerarán las actividades siguientes:

a) Prevenir que el acceso a los sistemas y bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

XXXIV. Órganos Autónomos: al Instituto Electoral del Estado de México, el Tribunal Electoral del Estado de México, la Comisión de Derechos Humanos del Estado de México, el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, la Fiscalía General de Justicia del Estado de México, las Universidades e Instituciones de Educación Superior dotadas de autonomía, y cualquier otro establecido en la Constitución Política del

Estado Libre y Soberano de México.

XXXV. Plataforma Nacional: a la Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública, que en términos del mismo, también comprenden los sistemas desarrollados, administrados, implementados y puestos en funcionamiento por el Instituto que le permitan cumplir con los procedimientos, obligaciones y disposiciones señaladas en la presente Ley.

XXXVI. Programa Nacional: al Programa Nacional de Protección de Datos Personales.

XXXVII. Programa Estatal: al Programa Estatal de Protección de Datos Personales.

XXXVIII. Programa de Cultura: al Programa de la Cultura de la Transparencia y de Protección de Datos Personales a que se refiere la Ley de Transparencia y Acceso a la Información Pública del Estado de México y sus Municipios.

XXXIX. Prueba de interés público: al proceso de ponderación entre el beneficio que reporta dar a conocer la información confidencial solicitada contra el daño que su divulgación genera en los derechos de las personas, llevado a cabo por el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, en el ámbito de sus respectivas competencias, fundarán y motivarán la orden de publicidad de los datos personales por motivos de interés público.

XL. Remisión: a la comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

XLI. Responsable: a los sujetos obligados a que se refiere la presente Ley que deciden sobre el tratamiento de los datos personales.

XLII. Seudonimización: al tratamiento de datos personales que no puedan atribuirse a un titular sin utilizar información adicional, cuando la información adicional figure por separado sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

XLIII. Sistema de datos personales: a los datos personales contenidos en los archivos de un sujeto obligado que puede comprender el tratamiento de una o diversas bases de datos para el cumplimiento de una o diversas finalidades.

XLIV. Sistema Nacional: al Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

XLV. Supresión: a la baja archivística de los datos personales, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

XLVI. Titular: a la persona física o jurídica colectiva que corresponden los datos personales que sean objeto de tratamiento.

XLVII. Tercero: a la persona física o jurídica colectiva, autoridad pública, servicio u organismo distinto de la o el titular, responsable, encargado, usuaria o usuario, destinataria o destinatario y las personas autorizadas para tratar los datos personales.

XLVIII. Transferencia: a la comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la o el titular, responsable o encargado.

XLIX. Transferente: al sujeto obligado que posee los datos personales objeto de la transferencia.

L. Tratamiento: a las operaciones efectuadas por los procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

LI. Usuarias o Usuarios: a las servidoras y los servidores públicos o personas físicas autorizadas para tratar los datos personales, distintos al responsable, al encargado y al administrador de los datos.

LII. Violación de la seguridad de los datos personales: a la violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transferidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, o cualquier otra que afecte la confidencialidad, integridad y disponibilidad de los datos personales. Se encuentran comprendidas dentro de este concepto las vulneraciones a las que hace referencia la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Aplicación de la Ley
Artículo 5. La presente Ley será aplicable a cualquier tratamiento de datos personales en posesión de sujetos obligados.

Derecho a la privacidad y limitaciones a la protección de datos personales
Artículo 6. El Estado garantizará la privacidad de los individuos y velará porque no se incurra en conductas que puedan afectarla arbitrariamente.

Los responsables aplicarán las medidas establecidas en esta Ley para la protección de las personas y su dignidad, respecto al tratamiento de sus datos personales.

El derecho a la protección de los datos personales solamente se limitará por razones de seguridad pública en términos de la Ley en la materia, disposiciones de orden público, salud pública o para proteger los derechos de terceros.

Datos personales sensibles
Artículo 7. Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso, inequívoco y explícito o en su defecto, se trate de los casos establecidos en el artículo 21 de la presente Ley.

Los datos personales sensibles y de naturaleza análoga en términos de las disposiciones legales aplicables estarán especialmente protegidos con medidas de seguridad de alto nivel.

Datos personales de niñas, niños y adolescentes
Artículo 8. En el tratamiento de datos personales de niñas, niños y adolescentes se privilegiará el interés superior de éstos, en términos de la Ley General de los Derechos de Niñas, Niños y Adolescentes, la Ley de Niñas, Niños y Adolescentes del Estado de México y las demás disposiciones legales aplicables, y se adoptarán las medidas idóneas para su protección.

El consentimiento se hará por conducto de la o el titular de la patria potestad o tutela, y el responsable del tratamiento obtendrá su autorización por escrito, así mismo verificará que el consentimiento fue dado o autorizado por la o el titular de la patria potestad o tutela sobre la niña, niño o adolescente.

No se publicarán los datos personales de niñas, niños y adolescentes, a excepción del consentimiento de su representante y no sea contraria al interés superior de la niñez.

Tratándose de obligaciones de transparencia o análogas, se publicará el nombre de la o el representante, acompañado del seudónimo del menor.

El responsable podrá limitar el acceso de la o el representante a los datos personales sensibles de adolescentes, en aquellos casos que se puedan afectar sus derechos humanos siempre y cuando no contravenga el interés superior.

Fuentes de acceso público
Artículo 9. Para los efectos de la presente Ley, se consideran fuentes de acceso público:

I. Los portales informativos o medios remotos y locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general.

II. Los directorios telefónicos en términos de la normativa específica.

III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa.

IV. Los medios de comunicación social.

V. Los registros públicos conforme a las disposiciones que les resulten aplicables.

La consulta la podrá hacer cualquier persona no impedida por una norma limitativa, o por el pago de una contraprestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.

Interpretación conforme
Artículo 10. La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto por la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales en los que el Estado mexicano sea parte, la Constitución Política del Estado Libre y Soberano de México, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia.

Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.

Supletoriedad
Artículo 11. A falta de disposición expresa en la presente Ley, se aplicarán de manera supletoria las disposiciones de la Ley General, la Ley General de Transparencia y Acceso a la Información Pública, de la Ley de Transparencia, del Código de Procedimientos Administrativos del Estado de México, el Código de Procedimientos Civiles del Estado de México y del Código Civil del Estado de México.

CAPÍTULO SEGUNDO
DEL PROGRAMA ESTATAL DE PROTECCIÓN DE DATOS PERSONALES

Coordinación y evaluación de las acciones relativas a la política pública transversal
Artículo 12. El Instituto para contribuir con lo que se mandata en el artículo 10 de la Ley General, coordinará y evaluará las acciones relativas a la política pública transversal de protección de datos personales en el ámbito estatal y municipal.

Vigilancia y respeto de la protección de datos personales en el orden estatal y municipal
Artículo 13. El Instituto contribuirá a mantener la plena vigencia y respeto del derecho a la protección de datos personales en el orden de gobierno estatal y municipal.

Las acciones coordinadas y cooperativas, así como el esfuerzo conjunto e integral, aportará al diseño, implementación y evaluación de la política pública; que con estricto apego a la normatividad aplicable en la materia; permita el ejercicio pleno y respeto del derecho a la protección de datos personales y la difusión efectiva de una cultura de este derecho y su accesibilidad.

Del programa Estatal
Artículo 14. El Instituto será responsable de diseñar, ejecutar y evaluar un Programa Estatal de Protección de Datos Personales que defina la política pública y establezca, como mínimo, objetivos, estrategias, acciones y metas; conforme a las bases siguientes:

I. Hacer del conocimiento general el derecho a la protección de datos personales;

II. Promover la educación y una cultura de protección de datos personales entre la sociedad mexiquense;

III. Fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición;

IV. Capacitar a los sujetos obligados en materia de protección de datos personales;

V. Certificar a los sujetos obligados, organizaciones o asociaciones de la sociedad, así como personas en general, que ofrezcan, en forma interdisciplinaria y profesional, la posibilidad de llevar a cabo cursos o talleres en materia de protección de datos personales;

VI. Impulsar la implementación y mantenimiento de un sistema de gestión de seguridad a que se hace referencia en la presente Ley, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia, y

VII. Prever los mecanismos que permitan medir, reportar y verificar las metas establecidas.

El Programa Estatal, se constituirá como un instrumento rector para la implementación de la política pública en materia de protección de datos personales en el Estado de México; asimismo, deberá determinar y jerarquizar los objetivos y metas que éste debe cumplir, así como definir las líneas de acción estratégicas que resulten necesarias.

El Programa Estatal, se evaluará objetiva, sistemática y anualmente, con respecto a las metas y los resultados de su ejecución, así como su incidencia en la consecución de la finalidad prevista en esta Ley. Con base en las evaluaciones correspondientes, el programa se modificará y/o adicionará al final de cada ejercicio anual y en la medida en que el Instituto lo estime necesario.

TÍTULO SEGUNDO
DE LOS PRINCIPIOS Y DISPOSICIONES APLICABLES AL TRATAMIENTO DE LA INFORMACIÓN

CAPÍTULO PRIMERO
DE LOS PRINCIPIOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Principios
Artículo 15 Los responsables en el tratamiento de datos personales, observarán los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad.

Principio de Calidad
Artículo 16. Los responsables adoptarán las medidas para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, para no alterar su veracidad.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por la o el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, serán suprimidos previo bloqueo y concluido su plazo de conservación.

Los plazos de conservación de los datos personales no excederán los necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, atendiendo a las disposiciones legales aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales, en términos de su catálogo de disposición documental.

Con el objeto de preservar la veracidad de la información, el responsable llevará una bitácora de las modificaciones que ha realizado a los registros de las usuarias y los usuarios de los sistemas y bases de datos personales, pudiendo conservar, los datos que se han referido inexactos, incompletos, incorrectos o desactualizados, los cuales inclusive podrán ser utilizados para efecto de responsabilidades.

Conservación, bloqueo y limitación del tratamiento
Artículo 17. El responsable establecerá y documentará los procedimientos para la conservación, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior.

El responsable establecerá los mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, llevará a cabo la limitación del tratamiento, para realizar una revisión periódica sobre la conservación de los datos personales.

Principio de Consentimiento
Artículo 18. El tratamiento de datos personales en posesión de los sujetos obligados contará con el consentimiento de su titular previo al tratamiento, salvo los supuestos de excepción previstos en la presente Ley y demás disposiciones legales aplicables.

El responsable demostrará que la o el titular consintió el tratamiento de sus datos personales.

El consentimiento será revocado en cualquier momento sin que se le atribuyan efectos retroactivos, en los términos previstos en la Ley. Para revocar el consentimiento, el responsable deberá realizar la indicación respectiva en el aviso de privacidad.

Elementos del consentimiento

Artículo 19. El consentimiento de la o el titular para el tratamiento de sus datos personales se otorgará de forma:

I. Libre: sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular,

II. Específica: refiere la finalidad concreta, lícita, explícita y legítima que justifique el tratamiento.

III. Informada: la o el titular tendrá conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

IV. Inequívoca: no admite duda o equivocación.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a Ley, se estará a lo dispuesto por el Código Civil del Estado de México.

Tipos de consentimiento
Artículo 20. El consentimiento podrá manifestarse de forma expresa o tácita.

El consentimiento será tácito cuando habiéndose puesto a disposición de la o el titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, salvo que la Ley o las disposiciones legales aplicables exijan que la voluntad del titular se manifieste expresamente.

El consentimiento será expreso cuando la voluntad de la o el titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, de acuerdo con la naturaleza del tratamiento, cuando así lo requiera una ley o los datos sean tratados para finalidades distintas. Cuando el tratamiento sea de datos personales sensibles, el consentimiento será expreso y por escrito.

El responsable obtendrá el consentimiento expreso y por escrito de la o el titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en esta Ley.

Excepciones al Principio de Consentimiento
Artículo 21. El responsable no estará obligado a recabar el consentimiento de la o el titular para el tratamiento de sus datos personales en los casos siguientes:

I. Lo establezca una disposición acordes con las bases, principios y disposiciones establecidas en esta Ley.

II. Las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó su tratamiento.

III. Exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.

IV. El reconocimiento o defensa de derechos de la o el titular ante autoridad competente.

V. Los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una

relación jurídica entre la o el titular y el responsable.

VI. Exista una situación de emergencia que pueda dañar a un individuo en su persona o en sus bienes.

VII. Los datos personales sean necesarios para el tratamiento de prevención, diagnóstico y la prestación de asistencia sanitaria.

VIII. Los datos personales figuren en fuentes de acceso público.

IX. Los datos personales se sometan de manera previa a procedimientos de anonimización, disociación o seudonimización, tendientes a evitar la asociación de los datos personales con su titular.

X. La o el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Principio de Finalidad
Artículo 22. Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, en los casos siguientes:

I. Cuente con atribuciones conferidas en ley y medie el consentimiento del titular.

II. Se trate de una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones legales aplicables.

Principio de Información
Artículo 23. El responsable tendrá la obligación de informar a través del aviso de privacidad de modo expreso, preciso e inequívoco a las y los titulares, la información que se recaba de ellos y con qué fines, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que puedan tomar decisiones informadas al respecto.

El aviso de privacidad estará redactado y estructurado de manera clara precisa y sencilla, será difundido por los medios electrónicos y físicos con que cuente el responsable.

Cuando resulte imposible dar a conocer a la o el titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable instrumentará medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional.

Principio de Lealtad
Artículo 24. El responsable no podrá obtener, recolectar, recabar, tratar, o transferir datos personales, a través de medios engañosos, fraudulentos desleales o ilícitos, privilegiando la protección de los intereses de privacidad de la o el titular de la información.

Principio de Licitud
Artículo 25. El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

El responsable podrá considerar los siguientes parámetros a fin de determinar si el tratamiento que

realiza es lícito:

a) La o el titular dio su consentimiento expreso y por escrito para el tratamiento de sus datos personales para uno o varios fines específicos.

b) La ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

c) El cumplimiento de una obligación legal aplicable al responsable.

d) La protección de intereses vitales de la o el titular o de otra persona física.

e) Cumplir con el interés público o en el ejercicio de poderes públicos conferidos al responsable.

f) La satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, cuando no prevalecen los intereses, los derechos y libertades fundamentales de la o el titular que requieran la protección de datos personales, en particular cuando el interesado sea un menor de edad.

Lo dispuesto en el inciso f) no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Principio de Proporcionalidad
Artículo 26. El responsable sólo deberá tratar los datos personales adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Principio de Responsabilidad
Artículo 27. El responsable cumplirá con los principios de protección de datos establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior cuando los datos fueren tratados por un encargado o tercero a solicitud del sujeto obligado.

El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer a la o el titular, será respetado en todo momento y por terceros que guarde alguna relación jurídica.

El responsable implementará los mecanismos previstos en la presente Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos y rendirá cuentas sobre el tratamiento de datos personales en su posesión a la o el titular y al Instituto, caso en el cual deberá observar la Constitución y los tratados internacionales en los que el Estado mexicano sea parte, en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

Mecanismos para demostrar el cumplimiento del principio de responsabilidad
Artículo 28. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales.

II. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones

y demás deberes en materia de protección de datos personales.

IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

V. Establecer un sistema de supervisión y vigilancia interna y/o externas, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás disposiciones legales aplicables.

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por diseño y por defecto con las obligaciones previstas en la presente Ley y las demás disposiciones legales aplicables.

CAPÍTULO SEGUNDO
DEL AVISO DE PRIVACIDAD

Comunicación del Aviso de Privacidad
Artículo 29. Los responsables pondrán a disposición de la o el titular en formatos impresos, digitales, visuales, sonoros o de cualquier otra tecnología, el aviso de privacidad, en las modalidades simplificado e integral.

Del Aviso de Privacidad Integral
Artículo 30. Cuando los datos hayan sido obtenidos personalmente de la o el titular, el aviso de privacidad integral deberá ser facilitado en el momento en el que se recabe el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiere facilitado el aviso con anterioridad, supuesto en el que podrá instrumentarse una señal de aviso para cumplir con el principio de responsabilidad.

Cuando los datos se obtengan de manera indirecta, el responsable adoptará los mecanismos necesarios para que la o el titular acceda al aviso de privacidad integral, salvo que exista constancia de que la o el titular ya fue informado del contenido del aviso de privacidad.

Contenido del Aviso de Privacidad Integral
Artículo 31. El aviso de privacidad integral contendrá la información siguiente:

I. La denominación del responsable.

II. El nombre y cargo del administrador, así como el área o unidad administrativa a la que se encuentra adscrito.

III. El nombre del sistema de datos personales o base de datos al que serán incorporados los datos personales.

IV. Los datos personales que serán sometidos a tratamiento, identificando los que son sensibles.

V. El carácter obligatorio o facultativo de la entrega de los datos personales.

VI. Las consecuencias de la negativa a suministrarlos.

VII. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento de la o el titular.

VIII. Cuando se realicen transferencias de datos personales se informará:

a) Destinatario de los datos.

b) Finalidad de la transferencia.

c) El fundamento que autoriza la transferencia.

d) Los datos personales a transferir.

e) Las implicaciones de otorgar, el consentimiento expreso.

Cuando se realicen transferencias de datos personales que requieran consentimiento, se acreditará el otorgamiento.

IX. Los mecanismos y medios estarán disponibles para el uso previo al tratamiento de los datos personales, para que la o el titular, pueda manifestar su negativa para la finalidad y transferencia que requieran el consentimiento de la o el titular.

X. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO, indicando la dirección electrónica del sistema para presentar sus solicitudes.

XI. La indicación por la cual la o el titular podrá revocar el consentimiento para el tratamiento de sus datos, detallando el procedimiento a seguir para tal efecto.

XII. Cuando aplique, las opciones y medios que el responsable ofrezca a las o los titulares para limitar el uso o divulgación, o la portabilidad de datos.

XIII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad,

XIV. El cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.

XV. El domicilio del responsable, y en su caso, cargo y domicilio del encargado, indicando su nombre o el medio por el cual se pueda conocer su identidad.

XVI. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento.

XVII. El procedimiento para que se ejerza el derecho a la portabilidad.

XVIII. El domicilio de la Unidad de Transparencia.

XIX. Datos de contacto del Instituto, incluidos domicilio, dirección del portal informativo, correo

electrónico y teléfono del Centro de Atención Telefónica, para que la o el titular pueda recibir asesoría o presentar denuncias por violaciones a las disposiciones de la Ley.

Del Aviso de Privacidad Simplificado
Artículo 32. Cuando los datos sean obtenidos directamente de la o el titular, por cualquier medio electrónico, óptico, sonoro, visual o a través de cualquier otra tecnología, el aviso de privacidad será puesto a disposición en lugar visible, previendo los medios o mecanismos para que la o el titular conozca el texto completo del aviso.

La puesta a disposición del aviso de privacidad, no exime al responsable de su obligación de proveer los mecanismos para que la o el titular pueda conocer el contenido del aviso de privacidad integral**.**

Contenido del Aviso de Privacidad Simplificado
Artículo 33. El aviso de privacidad simplificado deberá contener, al menos, la información a que se refieren las fracciones I, VII, VIII y IX del artículo relativo al contenido del aviso de privacidad integral.

Excepciones para la comunicación previa del Aviso de Privacidad
Artículo 34. No será necesario proporcionar el aviso de privacidad de manera previa, a la o el titular, cuando:

I. Expresamente una ley lo prevea.

II. Los datos personales se obtengan de manera indirecta.

III. Se trate de urgencias médicas, seguridad pública, o análogas en las cuales se ponga en riesgo la vida o la libertad de las personas, en términos de la legislación de la materia.

IV. Resulte imposible dar a conocer a la o el titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, en tales casos, el responsable instrumentará medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emitan el Instituto y el Sistema Nacional.

En el supuesto previsto en la fracción II del presente artículo, cuando los datos personales se obtengan de manera indirecta, es decir, no hayan sido obtenidos personal o directamente de su titular y el tratamiento tenga una finalidad diversa a la que originó su obtención, el responsable deberá comunicar el aviso de privacidad dentro de los tres meses siguientes al momento del registro de los datos, salvo que exista constancia de que la o el titular ya fue informado del contenido del aviso de privacidad por el transferente.

En los demás casos, es decir, cuando la finalidad sea análoga y compatible con aquella que originó su tratamiento conforme lo señalado en la presente Ley, el aviso de privacidad será comunicado al titular en los mismos términos del párrafo anterior.

CAPÍTULO TERCERO
DE LOS SISTEMAS Y EL TRATAMIENTO DE DATOS PERSONALES

Sistemas de Datos Personales
Artículo 35. Corresponde a cada sujeto obligado determinar, a través de su titular, órgano competente o Comité de Transparencia, la creación, modificación o supresión de sistemas y bases de datos personales, conforme a su respectivo ámbito de competencia.

De manera conjunta con la creación del sistema de datos personales, deberá emitirse el acuerdo que los clasifique con carácter confidencial, precisando además los datos que tienen el carácter no confidencial, acuerdo que deberá cumplir con lo dispuesto por la Ley de Transparencia. El acuerdo de clasificación al que hace referencia el presente párrafo servirá de soporte para la emisión de versiones públicas, sólo podrá ser modificado con motivo de acciones correctivas y preventivas a propuesta del administrador.

Tratamiento de los Sistemas de Datos Personales
Artículo 36. La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:

I. Cada sujeto obligado deberá informar al Instituto sobre la creación, modificación o supresión de sus sistemas de datos personales.

II. En caso de creación o modificación de sistemas de datos personales, se incluirá en el registro, los datos previstos la presente Ley.

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.

El registro de Sistemas de Datos Personales deberá realizarse a más tardar dentro de los seis meses siguientes al inicio del tratamiento por parte del responsable.

Registro de Sistemas de Datos Personales
Artículo 37. Los sujetos obligados registrarán ante el Instituto los sistemas de datos personales que posean. El registro deberá indicar por lo menos los datos siguientes:

I. El sujeto obligado que tiene a su cargo el sistema de datos personales.

II. La denominación del sistema de datos personales, la base de datos y el tipo de datos personales objeto de tratamiento.

III. El nombre y cargo del administrador, así como el área o unidad administrativa a la que se encuentra adscrito.

IV. El nombre y cargo del encargado.

V. La normatividad aplicable que dé fundamento al tratamiento en términos de los principios de finalidad y licitud.

VI. La finalidad del tratamiento.

VII. El origen, la forma de recolección y actualización de datos.

VIII. Datos transferidos, lugar de destino e identidad de los destinatarios, en el caso de que se registren transferencias.

IX. El modo de interrelacionar la información registrada, o en su caso, la trazabilidad de los datos en el sistema de datos personales.

X. El domicilio de la Unidad de Transparencia, así como de las áreas o unidades administrativas ante las que podrán ejercitarse de manera directa los derechos ARCO.

XI. El tiempo de conservación de los datos.

XII. El nivel de seguridad.

XIII. En caso de que se hubiera presentado una violación de la seguridad de los datos personales se indicará la fecha de ocurrencia, la de detección y la de atención. Dicha información deberá permanecer en el registro un año calendario posterior a la fecha de su atención.

Dicha información será publicada en el portal informativo del Instituto y se actualizará por la Unidad de Transparencia en el primer y séptimo mes de cada año.

TÍTULO TERCERO
DE LOS DEBERES Y LAS MEDIDAS DE SEGURIDAD

CAPÍTULO PRIMERO
DE LOS DEBERES

Medidas de seguridad administrativas, físicas y técnicas
Artículo 38. Con independencia del tipo de sistema y base de datos en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable adoptará, establecerá, mantendrá y documentará las medidas de seguridad administrativas, físicas y técnicas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, a través de controles y acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transferencia, acceso o cualquier tratamiento no autorizado o ilícito, de conformidad con lo dispuesto en los lineamientos que al efecto se expidan.

Principios y Deberes de los Datos Personales que deben ser preservadas
Artículo 39. En el tratamiento aplicarán medidas técnicas y administrativas apropiadas, así como observar deberes para garantizar un nivel de seguridad adecuado al riesgo, tales como:

I. Observar los deberes de confidencialidad, integridad y disponibilidad de los datos personales. Así mismo, la preservación de otros deberes como la autenticidad, no repudio y la confiabilidad que pueden resultar exigibles de acuerdo a la finalidad del tratamiento.

II. La disociación, anonimización y el cifrado de datos personales.

III. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

IV. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Deber de Confidencialidad
Artículo 40. Confidencialidad a la propiedad o característica consistente en que la información no se pondrá a disposición, ni se revelará a individuos, entidades o procesos no autorizados, por consiguiente, el responsable, el administrador, el encargado o en su caso las usuarias y los usuarios

autorizados son los únicos que pueden llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

El responsable, el encargado, las usuarias o los usuarios o cualquier persona que tenga acceso a los datos personales están obligados a guardar el secreto y sigilo correspondiente, conservando la confidencialidad aún después de cumplida su finalidad de tratamiento.

El administrador, el encargado o en su caso las usuarias y los usuarios autorizados son los únicos que pueden llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

El responsable establecerá controles o mecanismos que tengan por objeto que las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el sujeto obligado en los mismos términos que operen las prescripciones en materia de responsabilidades, salvo disposición legal en contrario.

En caso de contravención al deber de confidencialidad se estará a lo dispuesto por los ordenamientos administrativos correspondientes, independientemente de las acciones penales o civiles que en su caso procedan.

Deber de Integridad y de Disponibilidad de los Datos Personales
Artículo 41. El deber de integridad consiste en que los datos personales no serán alterados de manera no autorizada.

La disponibilidad es la propiedad de los datos personales de ser accesibles y utilizables cuando sean requeridos por personas, entidades o procesos autorizados.

Las medidas de seguridad establecidas en esta Ley para preservar la integridad y disponibilidad de los datos personales se integrarán con las establecidas en materia de archivos.

Deber de Autenticidad, No Repudio y Confiabilidad
Artículo 42. La autenticidad es la propiedad inherente a la veracidad del dato personal, es decir, que el dato personal es lo que se afirma que es.
El no repudio consiste en la capacidad de acreditar la ocurrencia o existencia de un evento o acción relacionada con el dato personal y la persona, entidad o proceso de origen.

La confiabilidad es la propiedad relativa a que los datos personales produzcan el funcionamiento y resultados esperados.

Las medidas de seguridad señaladas en este artículo se llevarán de conformidad con las disposiciones de la Ley de Gobierno Digital del Estado de México y Municipios, en congruencia con las normas técnicas que correspondan.

CAPÍTULO SEGUNDO
DE LAS MEDIDAS DE SEGURIDAD

Naturaleza de las medidas de seguridad y registro del nivel de seguridad
Artículo 43. Las medidas de seguridad previstas en este capítulo constituyen mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayor garantía en la protección y resguardo de los sistemas y bases de datos personales. Por la naturaleza de

la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.

El responsable y el encargado establecerán medidas para garantizar que cualquier persona que actúe bajo la autoridad de éstos y que tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones del responsable y observando lo previsto en la normatividad aplicable.

Las medidas de seguridad que al efecto se establezcan indicarán el nombre y cargo del administrador o usuaria o usuario, según corresponda. Cuando se trate de usuarias o usuarios se incluirán los datos del acto jurídico mediante el cual, el sujeto obligado otorgó el tratamiento del sistema de datos personales.

En el supuesto de actualización de estos datos, la modificación respectiva se notificará al Instituto en sus oficinas o en el portal que para tal efecto se cree, dentro de los treinta días hábiles siguientes a la fecha en que se efectuó.

El responsable o el encargado, designarán a una o un administrador, quien tendrá bajo su responsabilidad directa la base y sistema de datos personales.

Tipos y Niveles de Seguridad
Artículo 44. El responsable adoptará las medidas de seguridad, conforme a lo siguiente:

A. Tipos de seguridad:

I. Física: a la medida orientada a la protección de instalaciones, equipos, soportes, sistemas o bases de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

II. Lógica: a las medidas de seguridad administrativas y de protección que permiten la identificación y autenticación de las usuarias y los usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.

III. De desarrollo y aplicaciones: a las autorizaciones con las que contará la creación o tratamiento de los sistemas o bases de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de las usuarias y 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: a la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la seguridad de la información.

V. De comunicaciones y redes: a las medidas de seguridad técnicas, así como restricciones preventivas y de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

B. Niveles de seguridad:

I. Básico: a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases 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 las bases o sistemas de datos personales.

c) Registro de incidencias.

d) Identificación y autenticación.

e) Control de acceso.

f) Gestión de soportes.

g) Copias de respaldo y recuperación.

II. Medio: a la adopción de medidas de seguridad cuya aplicación corresponde a bases o sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los 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 aspectos siguientes:

a) Responsable de seguridad.

b) Auditoría.

c) Control de acceso físico.

d) Pruebas con datos reales.

III. Alto: a las medidas de seguridad aplicables a bases o 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 pública, prevención, investigación y persecución de delitos. En estos casos, 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.

c) Telecomunicaciones.

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

Elementos a considerar para la adopción de medidas de seguridad y su naturaleza
Artículo 45. Las medidas de seguridad adoptadas por el responsable considerarán:

I. El riesgo inherente a los datos personales tratados.

II. La sensibilidad de los datos personales tratados.

III. El desarrollo tecnológico.

IV. Las posibles consecuencias de una vulneración para las y los titulares.

V. Las transferencias de datos personales que se realicen.

VI. El número de titulares.

VII. Las violaciones a la seguridad previas ocurridas en los sistemas de tratamiento.

VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Actividades interrelacionadas para establecer y mantener las medidas de seguridad
Artículo 46. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable realizará, al menos, las actividades interrelacionadas siguientes:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

III. Elaborar un inventario de datos personales y de las bases y o sistemas de tratamiento.

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulnerabilidades a las que están sujetos los datos personales.

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Exigibilidad de Documentos y Registros derivados de un Sistema de Gestión de la Protección de Datos
Artículo 47. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales serán documentadas y contenidas en un sistema de gestión.

Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones legales aplicables.

Obligatoriedad del Documento de Seguridad
Artículo 48. Los sujetos obligados elaborarán y aprobarán un documento que contenga las medidas de

seguridad aplicables a las bases y sistemas de datos personales, tomando en cuenta los estándares internacionales de seguridad, la presente Ley así como los lineamientos que se expidan.

El documento de seguridad será de observancia obligatoria para los responsables, encargados y demás personas que realizan algún tipo de tratamiento a los datos personales. A elección del sujeto obligado, éste podrá ser único e incluir todos los sistemas y bases de datos personales que posea, por unidad administrativa en que se incluyan los sistemas y bases de datos personales en custodia, individualizado para cada sistema, o mixto.

Contenido del Documento de Seguridad
Artículo 49. El documento de seguridad deberá contener como mínimo lo siguiente:

I. Respecto de los sistemas de datos personales:

a) El nombre.

b) El nombre, cargo y adscripción del administrador de cada sistema y base de datos.

c) Las funciones y obligaciones del responsable, encargado o encargados y todas las personas que traten datos personales.

d) El folio del registro del sistema y base de datos.

e) El inventario o la especificación detallada del tipo de datos personales contenidos.

f) La estructura y descripción de los sistemas y bases de datos personales, lo cual consiste en precisar y describir el tipo de soporte, así como las características del lugar donde se resguardan.

II. Respecto de las medidas de seguridad implementadas deberá incluir lo siguiente:

a) Transferencia y remisiones.

b) Resguardo de soportes físicos y electrónicos.

c) Bitácoras para accesos, operación cotidiana y violaciones a la seguridad de los datos personales.

d) El análisis de riesgos.

e) El análisis de brecha.

f) Gestión de incidentes.

g) Acceso a las instalaciones.

h) Identificación y autenticación.

i) Procedimientos de respaldo y recuperación de datos.

j) Plan de contingencia.

k) Auditorías.

l) Supresión y borrado seguro de datos.

m) El plan de trabajo.

n) Los mecanismos de monitoreo y revisión de las medidas de seguridad.

o) El programa general de capacitación.

Revisión y actualización del documento de seguridad
Artículo 50. El responsable revisará el documento de seguridad de manera periódica y actualizarlo cuando ocurran los eventos siguientes:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.

IV. Implementación de acciones correctivas y preventivas ante una violación de la seguridad de los datos personales.

CAPÍTULO TERCERO
DE LAS VIOLACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES

Plan de Contingencia y Plan de Trabajo
Artículo 51. En caso de que ocurra una violación a la seguridad de los datos personales, el responsable implementará las acciones definidas en su plan de contingencia.

De manera posterior y durante la ocurrencia de los efectos de la violación a la seguridad de los datos personales, el responsable analizará las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso, a efecto de evitar que la violación se repita.

Supuestos que constituyen violación a la seguridad de los datos personales
Artículo 52. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como violaciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

I. La pérdida, robo, extravío.

II. La copia o destrucción no autorizada.

III. El uso o tratamiento no autorizado.

IV. El daño, la alteración o modificación no autorizada.

De la Bitácora de Violaciones a la Seguridad de los Datos Personales

Artículo 53. El responsable llevará una bitácora de las violaciones a la seguridad, de manera conjunta o separada con la bitácora de incidentes, en la que se describa la violación, la fecha en que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

De la Notificación ante Violaciones a la Seguridad de los datos personales
Artículo 54. En caso de violación a la seguridad de los datos personales que afecten de forma significativa los derechos patrimoniales o morales, el responsable deberá notificarlo al titular y al Instituto sin dilación alguna y de ser posible, a más tardar setenta y dos horas después de que se confirme que ocurrió la violación.

En tales casos, el responsable tomará las acciones encaminadas a detonar un proceso de revisión exhaustivo de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Si la violación fue cometida en los sistemas y bases de datos cuyo tratamiento corresponde al encargado externo, notificará inmediatamente al responsable, una vez confirmada la transgresión, a fin de que éste último proceda conforme a lo establecido en el presente artículo.

Fuera de los supuestos establecidos en el párrafo anterior, una vez atendida la violación a la seguridad, el responsable deberá registrar el incidente en la bitácora correspondiente, a fin de establecer acciones preventivas o correctivas e incorporarlas al Plan de Trabajo.

Contenido de la Notificación
Artículo 55. El responsable deberá informar al titular al menos lo siguiente:

I. La naturaleza del incidente.

II. Los datos personales comprometidos.

III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.

IV. Las acciones correctivas realizadas de forma inmediata.

V. Los medios donde puede obtener más información al respecto.

TÍTULO CUARTO
DE LA RELACIÓN DEL RESPONSABLE Y EL ENCARGADO

CAPÍTULO ÚNICO
DE LA RELACIÓN ENTRE EL RESPONSABLE Y EL ENCARGADO

Limitación de la Actuación del Encargado
Artículo 56. El encargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable.

El encargado deberá informar del tratamiento realizado a nombre y por cuenta del responsable en los términos y modalidades que determine este último.

Responsabilidad ante el incumplimiento por parte de encargadas o encargados

Artículo 57. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.

El encargado será responsable de las violaciones a la seguridad de los datos personales cuando éstas deriven del incumplimiento de las instrucciones del responsable.

Formalidad de la relación con el encargado
Artículo 58. La relación entre el responsable y el encargado deberá estar formalizada a través de contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable y que permita acreditar su existencia, alcance y contenido.

En el contrato o instrumento jurídico que decida el responsable se deberá prever al menos, que las cláusulas generales relacionadas con los servicios que preste el encargado sean las siguientes:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.

III. El nivel de protección requerido para los datos de acuerdo con su naturaleza.

IV. La implementación de las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

V. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

VI. Guardar confidencialidad respecto de los datos personales tratados.

VII. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

VIII. Abstenerse de transferir los datos personales salvo en el caso que el responsable así lo determine, o la comunicación derive de una subcontratación o por mandato expreso de la autoridad competente.

IX. Las responsabilidades y penalizaciones que correspondan por el uso inadecuado de los datos.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la presente Ley y demás disposiciones legales aplicables, así como lo establecido en el aviso de privacidad correspondiente.

Subcontratación de servicios por encargados
Artículo 59. El encargado podrá a su vez, subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie la autorización expresa de este último. El subcontratado también asumirá el carácter de encargado en los términos de la presente la Ley y demás disposiciones legales que resulten aplicables en la materia.

Cuando el contrato o el instrumento jurídico a través del cual se haya formalizado la relación entre el responsable y el encargado, prevea que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el párrafo anterior se entenderá como otorgada a través de lo estipulado en éstos.

El subcontratado deberá contar con experiencia y capacidad profesional para el desempeño de las responsabilidades a desarrollar.

Una vez obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que decida, de conformidad con la normatividad que le resulte aplicable y permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en el presente capítulo.

Formalizada la relación entre el subcontratado y el encargado, éste último deberá notificarlo de manera inmediata, proporcionando copia del instrumento jurídico correspondiente.

Encargado que brinda servicios, aplicaciones e infraestructura de cómputo en la nube
Artículo 60. El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones legales que resulten aplicables en la materia.

En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Requisitos que debe cumplir el Proveedor de Cómputo en la Nube
Artículo 61. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos a través de condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla al menos, con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable.

b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.

c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.

d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

II. Cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.

b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.

c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.

d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al

responsable y que este último haya podido recuperarlos.

e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la presente Ley y demás disposiciones legales que resulten aplicables en la materia.

TÍTULO QUINTO
DE LAS TRANSFERENCIAS Y REMISIONES

CAPÍTULO ÚNICO
DISPOSICIONES APLICABLES A LAS TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES

Disposiciones específicas para transferencias y remisiones
Artículo 62. Las disposiciones del presente capítulo se aplicaran a fin de asegurar que el nivel de protección de los datos personales garantizados en la presente Ley no se vea menoscabado, las transferencias constituyen una categoría especial de tratamiento de datos personales, en términos de las disposiciones especiales previstas en este capítulo.

Toda transferencia de datos personales, sea nacional o internacional, se encuentra sujeta al consentimiento expreso de su titular, salvo las excepciones previstas en la presente Ley, en éste último supuesto, el transferente podrá notificar de manera general o en supuestos especiales y siempre y cuando no contravenga lo establecido por las leyes especiales de la materia que corresponda, a fin que el titular esté en posibilidad de ejercer sus derechos ARCO ante el destinatario.

Se entenderá que el titular de los datos otorgó su consentimiento expreso cuando en el documento respectivo se incluya su firma autógrafa, su firma electrónica avanzada o su sello electrónico. Los sujetos obligados deberán cumplir con las disposiciones aplicables en materia de certificados digitales o firmas electrónicas avanzadas, estipuladas en la Ley de Gobierno Digital del Estado de México y Municipios, su Reglamento, así como en las demás disposiciones aplicables a la materia.

No se considerarán transferencias las remisiones, ni la comunicación de datos entre áreas o unidades administrativas adscritas al mismo sujeto obligado en el ejercicio de sus atribuciones.

Las remisiones nacionales e internacionales no requerirán ser informadas al titular, ni contar con su consentimiento.

El responsable podrá establecer medidas de control para identificar la información sujeta a transferencia y remisión que permitan atribuir su uso a una persona u organización específica, para deslindar eventuales responsabilidades. El responsable no estará obligado a informar las medidas de control utilizadas a los destinatarios o encargados, pero si estará obligado a demostrar de manera objetiva la forma en que es atribuible a una persona u organización en particular.

Formalización de la transferencia
Artículo 63. Toda transferencia deberá formalizarse a través de la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento

de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Lo dispuesto en el párrafo anterior, no será aplicable en los casos siguientes:

I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.

II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de destinatario, siempre y cuando las facultades entre éste último y el transferente sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del transferente.

Condiciones para la transferencia o remisión
Artículo 64. El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional en los términos que señale la Ley General.

Aceptación del aviso de privacidad por parte del destinatario
Artículo 65. En toda transferencia de datos personales, el responsable deberá comunicar al destinatario el aviso de privacidad conforme al cual se tratan los datos personales frente al titular.

Cuando la transferencia sea nacional, el destinatario de los datos personales deberá comprometerse a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el transferente.

El transferente deberá demostrar que comunicó el aviso de privacidad, ante lo cual se presume que el destinatario conoce y acepta las condiciones del tratamiento.

Excepciones al consentimiento expreso en transferencias
Artículo 66. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los supuestos siguientes:

I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por los Estados Unidos Mexicanos.

II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última.

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados.

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el transferente y un tercero.

VIII. Cuando se trate de los casos en los que el transferente no esté obligado a recabar el consentimiento del titular para el tratamiento y transferencia de sus datos personales, conforme a lo dispuesto en el artículo relativo a las excepciones del principio de consentimiento.

IX. Cuando la transferencia sea necesaria por razones de seguridad pública.

La actualización de alguna de las excepciones previstas en este artículo, no exime al responsable de cumplir con las obligaciones previstas en el presente capítulo que resulten aplicables.

Transferencias entre entidades federativas
Artículo 67. En el ámbito nacional, tratándose de requerimientos efectuados con carácter urgente o vinculados a una medida de apremio, responsabilidad o sanción, el responsable deberá verificar que la autoridad requirente cuenta con atribuciones suficientes para llevar a cabo el tratamiento de datos personales, en estos casos, esta última será responsable por las violaciones a la seguridad de los datos personales que se llegaran a configurar con motivo de dicho requerimiento. Tratándose de datos que pudieran tener el carácter de sensibles, el responsable deberá notificar al titular dentro de los cinco días siguientes al en que se hubiera efectuado la transferencia.

En el supuesto que los destinatarios de los datos sean personas o instituciones de otras entidades, el transferente de datos personales deberá realizar la transferencia de los mismos, conforme a las disposiciones previstas en la legislación aplicable, siempre y cuando se garanticen los niveles de seguridad y protección previstos en la presente Ley y demás ordenamientos legales aplicables.

Al evaluar la adecuación del nivel de protección, el transferente tendrá en cuenta, en particular, respecto del destinatario los elementos siguientes:

a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación aplicable, tanto general como específica, incluida la relativa a cuestiones de seguridad y la legislación penal.

b) El acceso de las autoridades públicas a los datos personales, así como la legislación en materia de protección de datos y su aplicación, incluido lo referente a las transferencias de datos personales a otro país u organización internacional.

c) El reconocimiento a los titulares del derecho a la protección de éstos, así como la existencia de medios de impugnación en aquellos casos que sean violentados.

d) La jurisprudencia y criterios en materia de protección de datos personales.

e) La existencia y el funcionamiento efectivo de una o varias autoridades u organismos de control autónomos, responsables de garantizar y hacer cumplir la legislación en materia de protección de datos.

f) Los compromisos internacionales asumidos por el país, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

TÍTULO SEXTO

ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO ÚNICO
MEJORES PRÁCTICAS Y ACCIONES PREVENTIVAS

De las mejores prácticas
Artículo 68. Para el cumplimiento de las obligaciones previstas en la presente Ley, el responsable podrá adoptar o desarrollar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto:

I. Elevar el nivel de protección de los datos personales.

II. Armonizar el tratamiento de datos personales en un sector específico.

III. Facilitar el ejercicio de los derechos ARCO por parte de los titulares.

IV. Facilitar las transferencias de datos personales.

V. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales.

VI. Demostrar ante el Instituto el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

Validación o Reconocimiento de Mejores Prácticas
Artículo 69. Todo esquema de mejores prácticas que busque la validación o reconocimiento por parte del Instituto deberá:

I. Cumplir con los parámetros que para tal efecto emita el Instituto conforme a los criterios que fije el Sistema Nacional.

II. Ser notificado ante el Instituto de conformidad con el procedimiento establecido en los parámetros señalados en la fracción anterior, a fin que sean evaluados y en su caso, validados o reconocidos e inscritos en el registro al que refiere el último párrafo de este artículo.

El Instituto deberá emitir las reglas de operación de los registros en los que se inscribirán aquellos esquemas de mejores prácticas validados o reconocidos.

El Instituto podrá inscribir los esquemas de mejores prácticas que haya reconocido o validado en el registro administrado por el Instituto Nacional, de acuerdo con las reglas que fije este último.

De la Evaluación de Impacto en la Protección de Datos Personales
Artículo 70. Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta

Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de Impacto en la Protección de Datos Personales y presentarla ante el Instituto, quien podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

El contenido de la evaluación de impacto a la protección de datos personales deberá determinarse por

el Instituto, de conformidad con los criterios que para tal efecto emita el Sistema Nacional.

Supuestos que Implican Tratamiento Intensivo o Relevante de Protección de Datos Personales
Artículo 71. Para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:

I. Existan riesgos inherentes a los datos personales a tratar.

II. Se traten datos personales sensibles.

III. Se efectúen o pretendan efectuar transferencias de datos personales.

Tratamientos Intensivos o Relevantes determinados en criterios adicionales
Artículo 72. El Sistema Nacional podrán emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales, de conformidad con lo dispuesto en el artículo anterior, en función de:

I. El número de titulares.

II. El público objetivo.

III. El desarrollo de la tecnología utilizada.

IV. La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue.

Plazo para Solicitar Evaluación de Impacto en la Protección de Datos Personales
Artículo 73. Los sujetos obligados que realicen una Evaluación de Impacto en la Protección de Datos Personales, deberán presentarla ante el Instituto, treinta días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, a efecto que emitan las recomendaciones no vinculantes correspondientes.

Término para la emisión de la Evaluación de Impacto en la Protección de Datos Personales
Artículo 74. El Instituto deberá emitir, de ser el caso, recomendaciones no vinculantes sobre la Evaluación de Impacto en la Protección de Datos Personales presentado por el responsable.

El plazo para la emisión de las recomendaciones a que se refiere el párrafo anterior será dentro de los treinta días siguientes contados a partir del día siguiente a la presentación de la evaluación.

Excepción a la Evaluación de Impacto a en la Protección de Datos Personales
Artículo 75. Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la evaluación de impacto en la protección de datos personales.

TÍTULO SÉPTIMO
DEL TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE INSTANCIAS DE SEGURIDAD PÚBLICA, PROCURACIÓN Y ADMINISTRACIÓN DE JUSTICIA

CAPÍTULO ÚNICO
TRATAMIENTO DE DATOS PERSONALES POR INSTANCIAS DE SEGURIDAD PÚBLICA, PROCURACIÓN Y ADMINISTRACIÓN DE JUSTICIA

Obtención y tratamiento de datos por autoridades de Seguridad Pública
Artículo 76. La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de las sujetos obligados competentes en instancias de seguridad pública, procuración y administración de justicia, sin el consentimiento del titular, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en los sistemas y bases de datos establecidas para tal efecto.

Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente capítulo.

Cumplimiento de los principios establecidos en esta Ley
Artículo 77. En el tratamiento de datos personales así como en el uso de los sistemas y bases de datos para su almacenamiento, que realicen, los sujetos obligados competentes de las instancias de seguridad pública, procuración y administración de justicia deberán cumplir con los principios establecidos en la presente Ley.

Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.

Nivel de seguridad aplicable
Artículo 78. Los responsables a que se refiere este capítulo, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Sistemas de Datos Personales por Instituciones de Seguridad Pública
Artículo 79. Los sistemas y bases de datos personales creados para fines administrativos por las autoridades de seguridad pública estarán sujetos al régimen general de protección de datos personales previsto en la presente Ley y en la Ley de Seguridad del Estado de México.

TÍTULO OCTAVO
DE LAS INSTANCIAS DE COORDINACIÓN PARA LA PROTECCIÓN DE DATOS PERSONALES Y EL INSTITUTO

CAPÍTULO PRIMERO
DEL SISTEMA NACIONAL

Del Sistema Nacional
Artículo 80. El Sistema Nacional se conformará en los términos y de acuerdo con lo establecido en la Ley General de Transparencia y Acceso a la Información Pública.

El Instituto forma parte del Sistema Nacional, en el ámbito de su competencia y de conformidad con lo que al respecto establece la Ley General y la presente Ley.

CAPÍTULO SEGUNDO
DEL INSTITUTO COMO ORGANISMO GARANTE

Del Instituto
Artículo 81. El Instituto es la autoridad encargada de garantizar a toda persona la protección de sus datos personales que se encuentren en posesión de los sujetos obligados, a través de la aplicación de la presente Ley, en concordancia con lo establecido por las disposiciones legales y normatividad en la materia.

Atribuciones del Instituto
Artículo 82. El Instituto, además de las atribuciones encomendadas por la Ley de Transparencia y normatividad aplicable, tendrá las atribuciones siguientes:

I. Interpretar en el orden administrativo la presente Ley.

II. Orientar y asesorar a los particulares acerca de las solicitudes materia de esta Ley.

III. Conocer, sustanciar y resolver de los recursos de revisión interpuestos por los titulares o sus representantes, en términos de lo dispuesto en la presente Ley y demás disposiciones legales que resulten aplicables en la materia.

IV. Presentar petición fundada al Instituto Nacional, para que conozca de los recursos de revisión que por su interés y trascendencia así lo ameriten, en términos de lo previsto en la Ley General y demás disposiciones que resulten aplicables en la materia.

V. Proporcionar al Instituto Nacional los elementos que requiera para resolver los recursos de inconformidad que le sean presentados.

VI. Suscribir convenios de colaboración con el Instituto Nacional para el cumplimiento de los objetivos previstos en la presente Ley y demás disposiciones legales aplicables.

VII. Solicitar la cooperación del Instituto en los términos de la Ley General.

VIII. Administrar, en el ámbito de su competencia, la Plataforma Nacional de Transparencia.

IX. Interponer acciones de inconstitucionalidad en contra de leyes expedidas por la legislatura local, que vulneren el derecho a la protección de datos personales.

X. Establecer lineamientos, políticas, criterios y procedimientos en materia de protección de datos personales, así como para el manejo, tratamiento, seguridad y protección de los datos personales en posesión de los sujetos obligados en los supuestos que no estén expresamente previstos para el Sistema Nacional o la normatividad que derive del mismo.

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

XII. Llevar a cabo el Registro de los Sistemas de Datos Personales en posesión de los sujetos obligados.

XIII. Elaborar y actualizar el registro del nivel de seguridad aplicable a los sistemas y bases de datos

personales en posesión de las dependencias y entidades, así como establecer los estándares mínimos que deberán contener los documentos de seguridad de los sujetos obligados.

XIV. Formular observaciones y recomendaciones a los sujetos obligados que incumplan esta Ley.

XV. Emitir resoluciones y determinaciones.

XVI. Proporcionar apoyo técnico a los sujetos obligados y responsables en materia de protección de datos personales, así como celebrar con ellos, convenios de colaboración que contribuyan a la implementación de mejores prácticas.

XVII. Proporcionar a los sujetos obligados un sitio web tipo en el cual deberá estar disponible la información relativa a cualquier otra información que considere conveniente difundir en materia de protección de datos personales, así como sistemas informáticos que faciliten el cumplimiento de la presente Ley por parte de sujetos obligados y responsables.

XVIII. Participar a través del Sistema de Acceso, Rectificación, Cancelación y Oposición del Estado de México, en el desarrollo, administración, implementación y funcionamiento de la Plataforma Nacional, con objeto de atender los procedimientos establecidos en la presente Ley.

XIX. Elaborar guías y demás documentos para facilitar el cumplimiento de las disposiciones de esta Ley y el ejercicio de derechos ARCO de manera clara y sencilla.

XX. Emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de impacto en protección de datos personales que le sean presentadas.

XXI. Capacitar y certificar en materia de protección de datos personales en posesión de sujetos obligados en el ámbito material y territorial de competencia que le corresponde.

XXII. Verificar el cumplimiento de las disposiciones previstas en esta Ley a través de los procedimientos de revisión que resulten compatibles con las disposiciones de esta Ley.

XXIII. Implementar los procedimientos que resulten necesarios para el cumplimiento de las disposiciones de esta Ley y para asegurar la protección de datos personales de los titulares.

XXIV. Imponer las medidas de apremio para asegurar el cumplimiento de sus resoluciones.

XXV. Investigar las posibles violaciones a la seguridad de los datos personales a fin de determinar la práctica de verificaciones.

XXVI. Promover ante la autoridad que corresponda las responsabilidades y sanciones que se generen con motivo del incumplimiento a las disposiciones de esta Ley y demás normatividad aplicable.

XXVII. Hacer del conocimiento de las autoridades competentes, la probable responsabilidad derivada del incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones que resulten aplicables.

XXVIII. Procurar la conciliación entre las autoridades y los titulares de los datos personales en cualquier momento del procedimiento del Recurso de Revisión y en su caso, verificar el cumplimiento del acuerdo respectivo.

XXIX. Incluir en el informe anual de actividades que está obligado a presentar ante el Poder Legislativo

del Estado de México, en términos de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, un informe detallado en materia de protección de datos personales, que incluya la información a que hace referencia el artículo 84 de esta Ley.

XXX. Promover y difundir el ejercicio del derecho a la protección de datos personales.

XXXI. Promover entre las instituciones educativas públicas y privadas la cultura y difusión de protección de datos personales.

XXXII. Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales, así como de sus prerrogativas.

XXXIII. Elaborar y publicar estudios e investigaciones, así como organizar seminarios, cursos, talleres y demás actividades que permitan difundir y ampliar el conocimiento sobre la materia de esta Ley.

XXXIV. Notificar medidas precautorias no invasivas para la operación del área o unidad administrativa del responsable cuando se presuma la existencia de violaciones a la seguridad de los datos personales.

XXXV. Acceder sin restricciones a la información clasificada en posesión de los sujetos obligados para el cumplimiento de sus atribuciones.

XXXVI. Coordinarse con las autoridades competentes para que las solicitudes de ejercicio de derechos ARCO y los recursos de revisión presentados en lenguas indígenas, sean atendidos en la misma lengua.

XXXVII. Garantizar, en el ámbito de sus respectivas competencias, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.

XXXVIII. Aplicar indicadores y criterios para evaluar el desempeño de los responsables respecto del cumplimiento de la presente Ley y demás disposiciones que resulten aplicables.

XXXIX. Colaborar en el ámbito de su competencia, en el diseño, ejecución y evaluación del Programa Nacional de Protección de Datos Personales que señala la Ley General.

XL. Diseñar, ejecutar y evaluar el Programa Estatal y Municipal de Protección de Datos Personales.

XLI. Las demás que prevea esta Ley para el Instituto y normatividad aplicable, en concordancia con los que establece la Ley General.

Supervisión de la Protección
Artículo 83. Los responsables, encargados, administradores y cualquier persona que lleve a cabo tratamiento de datos personales deberán permitir a los servidores públicos del Instituto el acceso a la documentación técnica y administrativa de los mismos, a fin que pueda llevar a cabo las facultades de verificación del cumplimiento de la Ley.

Informe al Poder Legislativo del Estado de México
Artículo 84. El Instituto deberá incluir en su informe anual de actividades que está obligado a presentar ante el Poder Legislativo del Estado de México, en términos de la Ley de Transparencia, un informe detallado en materia de protección de datos personales, que incluya la información que le rindan los sujetos obligados, relativa, al menos, al número de solicitudes de acceso a datos personales

presentadas ante cada dependencia y entidad así como su resultado, su tiempo de respuesta, el número y resultado de los asuntos atendidos por el Instituto, un Informe de las visitas de verificación practicadas las actividades desarrolladas por el Instituto en la materia y las dificultades observadas en el cumplimiento de esta Ley, incluyendo la observancia a los principios de protección de datos personales por parte de los sujetos obligados. Para este efecto, el Instituto expedirá los lineamientos que considere necesarios.

De la cooperación y vinculación internacional
Artículo 85. El Instituto podrá establecer vínculos con otras autoridades de protección de datos personales o equivalentes, así como organizaciones, foros y agrupaciones de autoridades y profesionales en la materia, a fin intercambiar información, estrategias, experiencias y mejores prácticas, así como convenir mecanismos de cooperación y coordinación para la protección de datos personales entre connacionales, lo anterior, siempre y cuando no comprometa la seguridad pública del Estado de México o interfiera en negociaciones y relaciones internacionales.

Participación del Instituto en el Programa Nacional e integración al Programa de Cultura
Artículo 86. El Instituto participará en los términos y plazos que establezca el Sistema Nacional en el Programa Nacional.

Aspectos que debe contemplar el Programa de Cultura
Artículo 87. El Instituto, en el ámbito de su respectiva competencia o a través de los mecanismos de coordinación que al efecto se establezcan, deberá contemplar en el Programa de Cultura de la Transparencia y Protección de Datos Personales lo siguiente:

I. Promover la educación y una cultura de protección de datos personales entre la sociedad mexiquense.

II. Fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

III. Brindar capacitación y certificación a los sujetos obligados en materia de protección de datos personales.

IV. Proponer que en los programas y planes de estudio, libros y materiales que se utilicen en las instituciones educativas de todos los niveles y modalidades del Estado, se incluyan contenidos sobre el derecho a la protección de datos personales, así como una cultura sobre el ejercicio y respeto de éste.

V. Promover, entre las instituciones públicas y privadas de educación media superior y superior, la inclusión, dentro de sus programas de estudio, actividades académicas curriculares y extracurriculares en materia de protección de datos personales y cumplimiento de la normativa en la materia.

VI. Impulsar en conjunto con instituciones de educación básica y superior, la integración de centros de investigación, difusión y docencia sobre el derecho a la protección de datos personales que promuevan el conocimiento sobre este tema y coadyuven con el Instituto en sus tareas sustantivas.

VII. Proponer modelos para la implementación y mantenimiento de un sistema de gestión de seguridad de datos personales, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia.

VIII. Establecer, entre las instituciones públicas de educación, acuerdos para la elaboración y publicación de materiales que fomenten la cultura de la protección de datos personales.

IX. Promover, en coordinación con autoridades federales, estatales y municipales, la participación

ciudadana y de organizaciones sociales en talleres, seminarios y actividades que tengan por objeto la difusión de la protección de datos personales.

X. Desarrollar, programas de capacitación a titulares de este derecho para incrementar su ejercicio y aprovechamiento, privilegiando a integrantes de sectores vulnerables o marginados de la población.

XI. Impulsar, estrategias que pongan al alcance de los diversos sectores de la sociedad los medios para el ejercicio de los derechos ARCO y derechos relacionados en la materia, acordes a su contexto sociocultural.

XII. Desarrollar, con el concurso de centros comunitarios digitales y bibliotecas públicas, universitarias, gubernamentales y especializadas, programas para la asesoría y orientación de sus usuarios en el ejercicio de los derechos ARCO y derechos relacionados en la materia.

XIII. Fomentar la creación de espacios de participación social y ciudadana que estimulen el intercambio de ideas entre la sociedad, los órganos de representación ciudadana y los responsables.

XIV. Prever los mecanismos que permitan medir, reportar y verificar las metas establecidas.

XV. Establecer convenios y alianzas estratégicas con autoridades vinculadas en la materia en el Estado de México, en otras entidades federativas y a nivel federal, de terceros países u organismos internacionales para promover el tratamiento seguro de datos personales, así como mecanismos de cooperación para facilitar el cumplimiento de los principios y deberes que establece esta Ley a cargo de cualquier persona, organismo o entidad.

CAPÍTULO TERCERO
DE LOS CRITERIOS DE INTERPRETACIÓN

De los criterios de interpretación
Artículo 88. Una vez que hayan causado ejecutoria las resoluciones dictadas con motivo de los recursos que se sometan a su competencia, el Instituto podrá emitir los criterios de interpretación que estime pertinentes y que deriven de lo resuelto en los mismos, conforme a lo dispuesto en la Ley General y atendiendo a las reglas establecidas en la Ley de Transparencia y demás normativa aplicable.

CAPÍTULO CUARTO
DEL CENTRO DE ATENCIÓN TELEFÓNICA

Del Centro de Atención Telefónica
Artículo 89. El Instituto deberá brindar asesoría y orientación a particulares en materia de protección de datos personales en posesión de sujetos obligados de esta Ley a través del Centro de Atención Telefónica, por los medios que establece la Ley de Transparencia.

TÍTULO NOVENO
RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO ÚNICO
DE LA ORGANIZACIÓN DE LOS SUJETOS OBLIGADOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

De la Unidad de Transparencia
Artículo 90. Cada responsable contará con una Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia y demás normativa aplicable, que tendrá las funciones siguientes:

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales.

II. Gestionar las solicitudes para el ejercicio de los derechos ARCO.

III. Establecer mecanismos para asegurar que los datos personales sólo se entreguen a su titular o su representante debidamente acreditados.

IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables.

V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.

VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.

VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

VIII. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto.

Los sujetos obligados y los responsables de manera directa o a través del Instituto promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a solicitudes de derechos ARCO, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

En la designación del titular de la Unidad de Transparencia, el responsable estará a lo dispuesto en la Ley de Transparencia y demás normatividad aplicable.

Del Oficial de Protección de Datos Personales
Artículo 91. Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, deberán designar a un Oficial de Protección de Datos Personales, especializado en la materia, quien realizará las atribuciones señaladas en el artículo anterior y formará parte de la Unidad de Transparencia. Los demás responsables podrán designarlo cuando lo determinen necesario para el adecuado desempeño de sus funciones.

De los Requisitos para ser Oficial de Protección de Datos Personales
Artículo 92. El oficial de protección de datos personales deberá tener el perfil adecuado para el cumplimiento de las obligaciones que se derivan de la presente Ley, contar con el nivel administrativo, dentro de la organización del responsable, que le permita implementar políticas transversales en esta materia y deberá cumplir con los requisitos siguientes:

I. Contar con la certificación en materia de protección de datos personales que para tal efecto emita el Instituto.

II. Contar con experiencia en materia de protección de datos personales acreditable cuando menos de

un año.

Ejercicio de derechos por parte de personas con algún tipo de discapacidad o grupos vulnerables
Artículo 93. El responsable procurará que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales. El responsable adoptará ajustes razonables en congruencia con lo establecido en la Ley de Transparencia.

Del Comité de Transparencia
Artículo 94. Cada sujeto obligado contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y la Ley de Transparencia.

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales.

Para los efectos de la presente Ley y sin perjuicio de otras funciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las atribuciones siguientes:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia.

II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.

III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO.

IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia.

V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto.

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales.

VIII. Dar vista al órgano interno de control o instancia equivalente del responsable, en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales, incluyendo casos relacionados con la declaración de inexistencia que realicen los responsables.

IX. Podrá proponer políticas públicas para la promoción de la cultura en la materia.

Responsabilidad y colaboración para el cumplimiento de esta Ley
Artículo 95. Corresponde en principio al administrador el cumplimiento de las disposiciones previstas en esta Ley para el responsable, sin perjuicio que los titulares de las áreas o unidades administrativas que decidan sobre el tratamiento, contenido o finalidad de los Sistemas de Datos Personales, encargados, terceros, usuarias o usuarios y demás autoridades previstas en este capítulo incurran en responsabilidad solidaria.

Los responsables deberán colaborar con el Instituto para capacitar y actualizar de forma permanente a todos sus servidores públicos en materia de protección de datos personales, a través de la impartición de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.

De las Obligaciones del Responsable en Materia de Seguridad
Artículo 96. Con el objeto de garantizar la seguridad de los sistemas y bases de datos personales, el Responsable en Materia de Seguridad deberá:

I. Atender y vigilar el cumplimiento de las medidas de seguridad establecidas por el Instituto o por el responsable, que garanticen, cuando menos, la autenticidad, confidencialidad, disponibilidad e integridad de los datos personales.

II. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas o bases de datos personales.

III. Difundir la normatividad aplicable entre los usuarios involucrados en el manejo de los datos personales.

IV. Elaborar un plan de capacitación en materia de seguridad de datos personales.

V. Llevar el control de los datos que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transferencia de datos y sus destinatarios.

VI. Inscribir los sistemas y bases de datos personales en un Registro creado para tal efecto.

VII. Establecer procedimientos de control de acceso a la red que incluyan perfiles de usuarias o usuarios o grupos de usuarias o usuarios para el acceso restringido a las funciones y programas de los sistemas o bases de datos personales.

VIII. Aplicar procedimientos de respaldos de bases de datos.

IX. Notificar al Instituto y al Comité de transparencia, así como a los titulares de los datos personales, los incidentes relacionados con la conservación o mantenimiento de los sistemas y bases de datos personales previstos en los lineamientos que al efecto se expidan.

El Responsable en Materia de Seguridad deberá ser designado atendiendo preferentemente a sus conocimientos y experiencia en al menos una de las materias siguientes: administración de procesos, sistemas de gestión, procedimiento administrativo, seguridad de la información, gestión documental y administración pública.

TÍTULO DÉCIMO
DERECHOS DE LOS TITULARES Y SU EJERCICIO

CAPÍTULO PRIMERO
DERECHOS ARCO, PORTABILIDAD Y LIMITACIÓN DEL TRATAMIENTO

Derechos ARCO
Artículo 97. Los derechos de acceso, rectificación, cancelación y oposición de datos personales son

derechos independientes. El ejercicio de cualquiera de ellos no es requisito previo no impide el ejercicio de otro. La procedencia de estos derechos, en su caso, se hará efectiva una vez que el titular o su representante legal acrediten su identidad o representación, respectivamente.

En ningún caso el acceso a los datos personales de un titular podrá afectar los derechos y libertades de otros.

El ejercicio de cualquiera de los derechos ARCO, forma parte de las garantías primarias del derecho a la protección de datos personales.

Derecho de Acceso
Artículo 98. El titular tiene derecho a acceder, solicitar y ser informado sobre sus datos personales en posesión de los sujetos obligados, así como la información relacionada con las condiciones y generalidades de su tratamiento, tales como el origen de los datos, las condiciones del tratamiento del cual sean objeto, las cesiones realizadas o que se pretendan realizar, así como tener acceso al aviso de privacidad al que está sujeto el tratamiento y a cualquier otra generalidad del tratamiento, en los términos previstos en la Ley.

El responsable debe responder al ejercicio del derecho de acceso, tenga o no datos de carácter personal del interesado en su sistema de datos.

Derecho de Rectificación
Artículo 99. El titular tendrá derecho a solicitar la rectificación de sus datos personales cuando sean inexactos, incompletos, desactualizados, inadecuados o excesivos.

Será el responsable del tratamiento, en términos de los lineamientos que emita el Instituto, quien decidirá cuando la rectificación resulte imposible o exija esfuerzos desproporcionados.

La rectificación podrá hacerse de oficio, cuando el responsable del tratamiento tenga en su posesión los documentos que acrediten la inexactitud de los datos.

Cuando los datos personales hubiesen sido transferidos o remitidos con anterioridad a la fecha de rectificación, dichas rectificaciones deberán hacerse del conocimiento de los destinatarios o encargados, quienes deberán realizar también la rectificación correspondiente.

Derecho de Cancelación
Artículo 100. El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable a fin que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Sin perjuicio de lo que disponga la normatividad aplicable al caso concreto, el responsable procederá a la cancelación de datos, previo bloqueo de los mismos, cuando hayan transcurrido los plazos establecidos por los instrumentos de control archivísticos aplicables.

Cuando los datos personales hubiesen sido transferidos con anterioridad a la fecha de cancelación, dichas cancelaciones deberán hacerse del conocimiento de los destinatarios, quienes deberán realizar también la cancelación correspondiente.

Bloqueo del Dato
Artículo 101. La cancelación dará lugar al bloqueo de los datos en el que el responsable lo conservará precautoriamente para efectos de responsabilidades, hasta el plazo de prescripción legal o contractual de éstas.

Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base y sistemas de datos que corresponda.

La cancelación procederá de oficio cuando el administrador, en términos de lo establecido en los lineamientos respectivos, estime que dichos datos resultan inadecuados o excesivos o cuando haya concluido la finalidad para la cual fueron recabados.

Excepciones al Derecho de Cancelación
Artículo 102. El responsable no estará obligado a cancelar los datos personales cuando:

I. Deban ser tratados por disposición legal.

II. Se refieran a las partes de un contrato y sean necesarios para su desarrollo y cumplimiento.

III. Obstaculicen actuaciones judiciales o administrativas, la investigación y persecución de delitos o la actualización de sanciones administrativas, afecten la seguridad o salud pública, disposiciones de orden público, o derechos de terceros.

IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular o de un tercero.

V. Sean necesarios para realizar una acción en función del interés público.

VI. Se requieran para cumplir con una obligación legalmente adquirida por el titular.

Derecho de Oposición
Artículo 103. El titular tendrá derecho en todo momento y por razones legítimas a oponerse al tratamiento de sus datos personales, para una o varias finalidades o exigir que cese el mismo, en los supuestos siguientes:

I. Cuando los datos se hubiesen recabado sin su consentimiento y éste resultara exigible en términos de esta Ley y disposiciones aplicables.

II. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular.

III. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

IV. Cuando el titular identifique que se han asociado datos personales o se le ha identificado con un registro del cuál no sea titular o se le incluya dentro de un sistema de datos personales en el cual no tenga correspondencia.

V. Cuando existan motivos fundados para ello y la Ley no disponga lo contrario.

De la Portabilidad de Datos Personales
Artículo 104. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita

seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transferir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

El Instituto de conformidad con los criterios que fije el Sistema Nacional establecerá a través de lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

Cuando aplique, el responsable deberá establecer el procedimiento para la portabilidad en su aviso de privacidad.

De la Limitación del Tratamiento
Artículo 105. El titular tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) El titular impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.

b) El tratamiento sea ilícito y el titular se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.

c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

d) El titular se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular.

Cuando el tratamiento de datos personales se haya limitado en términos del inciso d) dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público determinado en las leyes.

Todo titular que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

El responsable deberá notificar cualquier modificación al tratamiento de los datos personales a cada destinatario o encargado a los que se hayan transferido o remitido los datos personales, salvo que sea imposible o exija esfuerzos desproporcionados.

CAPÍTULO SEGUNDO
DEL EJERCICIO DE DERECHOS ARCO Y LOS DERECHOS RELACIONADOS EN LA MATERIA

Legitimación para Ejercer los Derechos ARCO
Artículo 106. La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO, de portabilidad de los datos y limitación del tratamiento, se sujetará al procedimiento establecido en el

presente Título y demás disposiciones que resulten aplicables en la materia.

Los titulares o sus representantes legales podrán solicitar a través de la Unidad de Transparencia, en términos de lo que establezca la presente Ley, que se les otorgue acceso, rectifique, cancele, o que haga efectivo su derecho de oposición, respecto de los datos personales que le conciernan y que obren en un sistema de datos personales y base de datos en posesión de los sujetos obligados.

Para el ejercicio de los derechos ARCO solicitados será necesario acreditar la identidad de titular y en su caso la identidad y personalidad con la que actúe el representante.

Tratándose de datos personales concernientes a personas fallecidas o de quienes haya sido declarada judicialmente su presunción de muerte, la persona que acredite tener un interés jurídico de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido, o que exista un mandato judicial para dicho efecto.

El titular podrá autorizar dentro de una cláusula del testamento a las personas que podrán ejercer sus derechos ARCO al momento del fallecimiento.

El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

Gratuidad en el Ejercicio de los Derechos ARCO
Artículo 107. El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío en los términos previstos por el Código Financiero del Estado de México y Municipios y demás disposiciones jurídicas aplicables. En ningún caso el pago de derechos deberá exceder el costo de reproducción, certificación o de envío.

Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo al solicitante.

La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.

El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular.

Plazo de Respuesta, Ampliación y Negativa
Artículo 108. El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, privilegiando los mecanismos que faciliten su ejercicio de una manera breve y ágil. El plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular.

En caso que el responsable no emita respuesta a la solicitud de ejercicio de derechos ARCO se entenderá que la respuesta es negativa.

Modalidades de la Presentación de la Solicitud
Artículo 109. La presentación de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales se podrá realizar en cualquiera de las modalidades siguientes:

I. Por escrito libre presentado personalmente por el titular o su representante legal en la Unidad de Transparencia, o bien, en los formatos establecidos para tal efecto, o bien a través de correo ordinario, correo certificado o servicio de mensajería.

II. Verbalmente por el titular o su representante legal en la Unidad de Transparencia, la cual deberá ser capturada por el responsable en el formato respectivo.

III. Por el sistema electrónico que el Instituto o la normatividad aplicable establezca para tal efecto.

El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibo que corresponda.

El Instituto podrá establecer mecanismos adicionales, tales como formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.

Los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable.

Requisitos de Solicitudes para el Ejercicio de los Derechos ARCO
Artículo 110. La solicitud para el ejercicio de derechos ARCO, deberá contener:

I. El nombre del titular y su domicilio, o cualquier otro medio para recibir notificaciones.

II. Los documentos que acrediten la identidad del titular y en su caso, la personalidad e identidad de su representante.

III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud.

IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso.

V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular.

VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Tratándose del requisito de la fracción I, si es el caso del domicilio no se localiza dentro del Estado de

México, las notificaciones se efectuarán por estrados.

De manera adicional, el titular podrá aportar pruebas para acreditar la procedencia de su solicitud.

Tratándose de una solicitud de acceso a datos personales se señalará la modalidad en la que el titular prefiere se otorgue éste, la cual podrá ser por consulta directa, copias simples, certificadas, digitalizadas u otro tipo de medio electrónico.

El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

Prevención en caso de omisión de requisitos no subsanables
Artículo 111. En caso que la solicitud no satisfaga alguno de los requisitos a que se refiere el artículo anterior y el responsable no cuente con elementos para subsanarla, se prevendrá al titular de los datos o a su representante dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de derechos ARCO.

La prevención tendrá el efecto de interrumpir el plazo que tiene el responsable para dar respuesta a la solicitud de ejercicio de los derechos ARCO.

Incompetencia y Reconducción de Vía
Artículo 112. Cuando el responsable no sea competente para atender la solicitud para el ejercicio de derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud y en caso de poderlo determinar, orientarlo hacia el responsable competente.

En caso que el responsable advierta que la solicitud para el ejercicio de derechos ARCO corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento al titular en el plazo previsto en el primer párrafo.

Inexistencia de la información
Artículo 113. En caso que el responsable estuviere obligado a contar con los datos personales sobre los cuales se ejercen los derechos ARCO y declare su inexistencia en sus archivos, bases, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales.

Existencia de trámite específico
Artículo 114. Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, el responsable deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguiente a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto que este último decida si ejerce sus derechos a través del trámite específico, o bien a través del procedimiento para el ejercicio de los derechos ARCO.

La generación de nuevos datos, la realización de cálculos o el procesamiento a los datos personales no podrá obtenerse a través del ejercicio de derecho de acceso ya que éste implica, únicamente, obtener

del responsable los datos personales en la manera en la que obren en sus archivos y en el estado en que se encuentren.

Orientación al Titular para el Ejercicio de sus Derechos
Artículo 115. Los responsables deben de orientar en forma sencilla y comprensible a toda persona sobre los trámites y procedimientos que deben efectuarse para ejercer sus derechos ARCO, la forma de realizarlos, la manera de llenar los formularios que se requieran, así como de las instancias ante las que se puede acudir a solicitar orientación o formular quejas, consultas o reclamos sobre la prestación del servicio o sobre el ejercicio de las funciones o competencias a cargo de los servidores públicos que se trate.

El Instituto deberá adoptar mecanismos para orientar a los titulares sobre el ejercicio de derechos ARCO por vía telefónica.

Medios para Recibir Notificaciones
Artículo 116. Se presumirá que el titular acepta que las notificaciones le sean efectuadas por el mismo conducto que presentó su escrito, salvo que acredite haber señalado uno distinto para recibir notificaciones.

Los medios por los cuales el solicitante podrá recibir notificaciones o acuerdos serán: correo electrónico, a través del sistema electrónico instrumentado por el Instituto o notificación personal en su domicilio o en la Unidad de Transparencia que corresponda. En el caso que el solicitante no señale domicilio o éste no se ubique en el Estado de México o algún medio para oír y recibir notificaciones, el acuerdo o notificación se dará a conocer por lista que se fije en los estrados del Módulo de Acceso del sujeto obligado que corresponda.

Improcedencia de los derechos ARCO
Artículo 117. Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:

I. Cuando el titular o su representante no estén debidamente acreditados para ello.

II. Cuando los datos personales no se encuentren en posesión del responsable.

III. Cuando exista un impedimento legal.

IV. Cuando se lesionen los derechos de un tercero.

V. Cuando se obstaculicen actuaciones judiciales o administrativas.

VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos.

VII. Cuando la cancelación u oposición haya sido previamente realizada.

VIII. Cuando el responsable no sea competente.

IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular.

X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular.

La improcedencia a que se refiere este artículo podrá ser parcial si una parte de los datos solicitados no encuadra en alguna de las causales antes citadas, en cuyo caso los responsables efectuarán

parcialmente el acceso, rectificación, cancelación y oposición requerida por el titular.

En cualquiera de los supuestos mencionados en este artículo, el administrador analizará el caso y emitirá una respuesta fundada y motivada, la cual deberá notificarse al solicitante a través de la Unidad de Transparencia en el plazo de hasta veinte días al que se refiere el artículo 108 de la presente Ley.

En las respuestas a las solicitudes de derechos ARCO, las Unidades de Transparencia deberán informar al solicitante del derecho y plazo que tienen para promover el recurso de revisión.

Cumplimiento de la atención de solicitudes ARCO
Artículo 118. Las solicitudes de ejercicio de los derechos ARCO se darán por cumplidas a través de expedición de copias simples, copias certificadas, documentos en la modalidad que se hubiese solicitado, previa acreditación de la identidad y personalidad del solicitante o en su caso, ante la notificación de improcedencia de su solicitud.

Cuando se determine la procedencia del ejercicio de dichos derechos y éstos se encuentren a disposición del titular en la modalidad que haya escogido previa acreditación, la solicitud se entenderá atendida si el solicitante no acude dentro de los sesenta días posteriores a la notificación.

TÍTULO DÉCIMO PRIMERO
DE LOS MEDIOS DE IMPUGNACIÓN

CAPÍTULO PRIMERO
DISPOSICIONES APLICABLES A LOS MEDIOS DE IMPUGNACIÓN

Medios de interposición
Artículo 119. El titular o su representante podrán interponer un recurso de revisión ante el Instituto o bien, ante la Unidad de Transparencia del responsable que haya conocido de la solicitud, a través de los medios siguientes:

I. Por escrito libre en el domicilio del Instituto o en las oficinas habilitadas que al efecto establezcan.

II. Por correo certificado con acuse de recibo.

III. Por formatos que al efecto emita el Instituto.

IV. Por los medios electrónicos que para tal fin se autoricen.

V. Cualquier otro medio que al efecto establezca el Instituto.

Se presumirá que el titular acepta que las notificaciones le sean efectuadas por el mismo conducto que presentó su escrito, salvo que acredite haber señalado uno distinto para recibir notificaciones.

Medios para acreditar identidad
Artículo 120. El titular podrá acreditar su identidad a través de cualquiera de los medios siguientes:

I. Identificación oficial.

II. Firma electrónica avanzada o del instrumento electrónico que lo sustituya.

III. Mecanismos de autenticación autorizados por el Instituto o el Instituto Nacional publicados por acuerdo general en el periódico oficial "Gaceta del Gobierno" o en el Diario Oficial de la Federación.

La utilización de la firma electrónica avanzada o del instrumento electrónico que lo sustituya eximirá de la presentación de la copia del documento de identificación.

Formas para acreditar personalidad en representación
Artículo 121. Cuando el titular actúe a través de un representante, éste deberá acreditar su personalidad en los términos siguientes:

I. Si se trata de una persona física, a través de carta poder simple suscrita ante dos testigos anexando copia de las identificaciones de los suscriptores o instrumento público o declaración en comparecencia personal del titular y del representante ante el Instituto.

II. Si se trata de una persona jurídica colectiva, a través de instrumento público.

Interposición respecto a datos de personas fallecidas
Artículo 122. La interposición de un recurso de revisión de datos personales concernientes a personas fallecidas, podrá realizarla la persona que acredite tener un interés jurídico o legítimo.

Notificaciones en medios de impugnación
Artículo 123. En la sustanciación de los recursos de revisión las notificaciones que emita el Instituto surtirán efectos el mismo día en que se practiquen.

Las notificaciones podrán efectuarse:

I. Personalmente en los casos siguientes:

a) Se trate de la primera notificación.

b) Se trate del requerimiento de un acto a la parte que deba cumplirlo.

c) Se trate de la solicitud de informes o documentos.

d) Se trate de la resolución que ponga fin al procedimiento que se trate.

e) En los demás casos que disponga la ley.

II. Por correo certificado con acuse de recibo o medios digitales o sistemas autorizados por el Instituto o el Instituto Nacional y publicados a través de acuerdo general en el Diario Oficial de la Federación o en el periódico oficial "Gaceta del Gobierno", cuando se trate de requerimientos, emplazamientos, solicitudes de informes o documentos y resoluciones que puedan ser impugnadas.

III. Por correo postal ordinario o por correo electrónico ordinario cuando se trate de actos distintos de los señalados en las fracciones anteriores.

IV. Por estrados, cuando la persona a quien deba notificarse no sea localizable en su domicilio, se ignore éste o el de su representante.

Las notificaciones personales a que hace referencia la fracción I de este artículo se efectuarán a través de los sistemas autorizados por el Instituto, cuando las solicitudes se hubieren tramitado por dicho medio.

Cómputo de plazos y preclusión
Artículo 124. El cómputo de los plazos señalados en el presente Título comenzará a correr a partir del día siguiente a aquél en que haya surtido efectos la notificación correspondiente.

Concluidos los plazos fijados a las partes, se tendrá por perdido el derecho que dentro de ellos debió ejercitarse, sin necesidad de acuse de rebeldía por parte del Instituto.

Obligación de atender requerimientos del Instituto
Artículo 125. El titular, su representante, el responsable o cualquier autoridad deberán atender los requerimientos de información en los plazos y términos que el Instituto establezca, de conformidad con la Ley General.

Cuando el titular, el responsable, el administrador o cualquier autoridad se niegue a atender o cumplimentar los requerimientos, solicitudes de información y documentación, emplazamientos, citaciones o diligencias notificadas por el Instituto o facilitar la práctica de las diligencias que hayan sido ordenadas o entorpezca las actuaciones del Instituto, tendrán por perdido su derecho para hacerlo valer en algún otro momento del procedimiento y el Instituto tendrá por ciertos los hechos materia del procedimiento y resolverá con los elementos que disponga.

Pruebas admisibles en los Medios de Impugnación
Artículo 126. En la sustanciación de los recursos de revisión las partes podrán ofrecer las pruebas siguientes:

I. La documental pública.

II. La documental privada.

III. La inspección.

IV. La pericial.

V. La testimonial.

VI. La confesional, excepto tratándose de autoridades.

VII. Las imágenes fotográficas, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.

VIII. La presuncional legal y humana.

El Instituto podrá allegarse de los medios de prueba que considere necesarios, sin más limitación que las establecidas en la ley.

CAPÍTULO SEGUNDO
DEL RECURSO DE REVISIÓN

Procedimiento para Sustanciar los Recursos de Revisión
Artículo 127. A falta de disposición expresa en esta Ley, el recurso de revisión será tramitado de conformidad con los términos, plazos y requisitos señalados en la Ley de Transparencia.

Plazo para interponer recurso de revisión
Artículo 128. El titular, por sí mismo o a través de su representante, podrán interponer un recurso de revisión ante el Instituto o la Unidad de Transparencia del responsable que haya conocido de la solicitud para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta.

Transcurrido el plazo previsto para dar respuesta a una solicitud para el ejercicio de los derechos ARCO sin que se haya emitido ésta, el titular o en su caso, su representante podrán interponer el recurso de revisión dentro de los quince días siguientes al que haya vencido el plazo para dar respuesta.

Procedencia del Recurso de Revisión
Artículo 129. El recurso de revisión procederá en los supuestos siguientes:

I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables.

II. Se declare la inexistencia de los datos personales.

III. Se declare la incompetencia por el responsable.

IV. Se entreguen datos personales incompletos.

V. Se entreguen datos personales que no correspondan con lo solicitado.

VI. Se niegue total o parcialmente el acceso, rectificación, cancelación u oposición de datos personales o los derechos relacionados con la materia.

VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible.

IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales.

X. Se obstaculice el ejercicio de los derechos ARCO, a pesar que fue notificada la procedencia de los mismos.

XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO.

XII. Se considere que la respuesta es desfavorable a su solicitud.

XIII. En los demás casos que dispongan las leyes.

Contenido del escrito de recurso
Artículo 130. Los únicos requisitos exigibles en el escrito de interposición del recurso de revisión serán los siguientes:

I. El responsable y de ser posible, el área ante quien se presentó la solicitud para el ejercicio de los derechos ARCO.

II. El nombre del titular que recurre o su representante y en su caso, del tercero interesado, así como el domicilio en el Estado de México o medio que señale para recibir notificaciones.

III. La fecha en que fue notificada la respuesta al titular o bien, en caso de falta de respuesta la fecha de la presentación de la solicitud para el ejercicio de los derechos ARCO y demás derechos relacionados con la materia.

IV. El acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad.

V. En su caso, copia de la respuesta que se impugna y de la notificación correspondiente.

VI. Los documentos que acrediten la identidad del titular y en su caso, la personalidad e identidad de su representante.

Al recurso de revisión se podrán acompañar las pruebas y demás elementos que el titular o su representante considere procedentes someter a juicio del Instituto.

En ningún caso será necesario que el titular ratifique el recurso de revisión interpuesto.

De la conciliación
Artículo 131. Una vez admitido el recurso de revisión, el Instituto podrá buscar una conciliación entre el titular y el responsable.

De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto deberá verificar el cumplimiento del acuerdo respectivo.

Procedimiento de conciliación
Artículo 132. Admitido el recurso de revisión y sin perjuicio de lo dispuesto por la Ley General, el Instituto promoverá la conciliación entre las partes, de conformidad con el procedimiento siguiente:

I. El Instituto requerirá a las partes para que manifiesten, por cualquier medio, su voluntad de conciliar, en un plazo no mayor a siete días, contados a partir de la notificación de dicho acuerdo, mismo que contendrá un resumen del recurso de revisión y de la respuesta del responsable si la hubiere, señalando los elementos comunes y los puntos de controversia.

La conciliación podrá celebrarse presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el Instituto. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.

Queda exceptuado de la etapa de conciliación, cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley de los Derechos de Niñas, Niños y Adolescentes del Estado de México, vinculados con la presente Ley y su Reglamento, salvo que cuente con representación legal debidamente acreditada.

II. Aceptada la posibilidad de conciliar por ambas partes, el Instituto señalará el lugar o medio, día y hora para la celebración de una audiencia de conciliación, la cual deberá realizarse dentro de los diez días siguientes en que el Instituto haya recibido la manifestación de la voluntad de conciliar de ambas partes, en la que se procurará avenir los intereses entre el titular y el responsable.

El conciliador podrá, en todo momento en la etapa de conciliación, requerir a las partes que presenten en un plazo máximo de cinco días, los elementos de convicción que estime necesarios para la conciliación.

El conciliador podrá suspender cuando lo estime pertinente o a instancia de ambas partes la audiencia por una ocasión. En caso que se suspenda la audiencia, el conciliador señalará día y hora para su reanudación dentro de los cinco días siguientes.

De toda audiencia de conciliación se levantará el acta respectiva, en la que conste el resultado de la misma. En caso que el responsable o el titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa.

III. Si alguna de las partes no acude a la audiencia de conciliación y justifica su ausencia en un plazo de tres días, será convocado a una segunda audiencia de conciliación en el plazo de cinco días, en caso que no acuda a esta última, se continuará con el recurso de revisión. Cuando alguna de las partes no acuda a la audiencia de conciliación sin justificación alguna, se continuará con el procedimiento.

IV. De no existir acuerdo en la audiencia de conciliación, se continuará con el recurso de revisión.

V. De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes.

El recurso de revisión quedará sin materia y el Instituto, deberán verificar el cumplimiento del acuerdo respectivo.

VI. El cumplimiento del acuerdo dará por concluido la sustanciación del recurso de revisión, en caso contrario, el Instituto reanudará el procedimiento.

El plazo al que se refiere el artículo siguiente de la presente Ley será suspendido durante el periodo de cumplimiento del acuerdo de conciliación.

Plazo para resolver el Recurso de Revisión
Artículo 133. El Instituto resolverá el recurso de revisión en un plazo que no podrá exceder de cuarenta días, el cual podrá ampliarse hasta por veinte días por una sola vez.

Suplencia de la Deficiencia de la Queja
Artículo 134. Durante el procedimiento a que se refiere el presente Capítulo, el Instituto deberá aplicar la suplencia de la queja a favor del titular, siempre y cuando no altere el contenido original del recurso de revisión, ni modifique los hechos o peticiones expuestas en el mismo, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones.

Facultad del Instituto para Allegarse de Pruebas
Artículo 135. El Instituto tendrá acceso a la información contenida en los sistemas y bases de datos personales de los responsables que resulte indispensable para resolver el recurso. Dicha información deberá ser mantenida con carácter confidencial y no estará disponible en el expediente.

Prevención por la falta de requisitos en el escrito de interposición del recurso
Artículo 136. Si en el escrito de interposición del recurso de revisión el recurrente no cumple con alguno de los requisitos previstos en el artículo 130 de la presente Ley y el Instituto no cuente con elementos para subsanarlos, deberá requerir al recurrente, por una sola ocasión, la información que subsane las omisiones en un plazo que no podrá exceder de cinco días, contados a partir del día siguiente de la presentación del escrito.

El recurrente contará con un plazo que no podrá exceder de cinco días, contados a partir del día siguiente al de la notificación de la prevención, para subsanar las omisiones, con el apercibimiento que en caso de no cumplir con el requerimiento, se desechará el recurso de revisión.

La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver el recurso, por lo que comenzará a computarse a partir del día siguiente a su desahogo.

Sentido de las resoluciones
Artículo 137. Las resoluciones del Instituto podrán:

I. Sobreseer o desechar el recurso de revisión por improcedente.

II. Confirmar la respuesta del responsable.

III. Revocar o modificar la respuesta del responsable.

IV. Ordenar el acceso, rectificación, cancelación u oposición de los datos personales, en caso de omisión del responsable.

Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los responsables deberán informar al Instituto el cumplimiento de sus resoluciones en un plazo no mayor a tres días hábiles contados a partir de aquel en que se hubiera dado cumplimiento a la resolución.

Ante la falta de resolución por parte del Instituto se entenderá confirmada la respuesta del responsable.

Cuando el Instituto determine durante la sustanciación del recurso de revisión que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia, deberán hacerlo del conocimiento del órgano interno de control o de la instancia competente del responsable para que ésta inicie, en su caso, el Procedimiento de Responsabilidad respectivo.

Causales de improcedencia
Artículo 138. El recurso de revisión podrá ser desechado por improcedente cuando:

I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 128 de la presente Ley.

II. El titular o su representante no acrediten debidamente su identidad y personalidad de este último.

III. El Instituto haya resuelto anteriormente en definitiva sobre la materia del mismo.

IV. No se actualice alguna de las causales del recurso de revisión previstas en el artículo 129 de la presente Ley.

V. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el recurrente, o en su caso, por el tercero interesado, en contra del acto recurrido ante el Instituto.

VI. El recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos.

VII. El recurrente no acredite interés jurídico.

El desechamiento no implica la preclusión del derecho del titular para interponer ante el Instituto un nuevo recurso de revisión.

Causales de Sobreseimiento
Artículo 139. El recurso de revisión sólo podrá ser sobreseído cuando:

I. El recurrente se desista expresamente.

II. El recurrente fallezca.

III. Admitido el recurso de revisión, se actualice alguna causal de improcedencia en los términos de la presente Ley.

IV. El responsable modifique o revoque su respuesta de tal manera que el recurso de revisión quede sin materia.

V. Quede sin materia el recurso de revisión.

Notificación de las resoluciones
Artículo 140. El Instituto deberá notificar a las partes la resolución y publicar las versiones públicas correspondientes, a más tardar, al tercer día siguiente de su aprobación.

Definitividad de las resoluciones del Instituto para Sujetos Obligados
Artículo 141. Las resoluciones que emita el Instituto serán definitivas, inatacables, vinculantes y obligatorias para los sujetos obligados. Dichas resoluciones serán de plena jurisdicción, por lo que tendrán efectos de pleno derecho para todos los sujetos obligados.

Impugnación de las Resoluciones por parte de Particulares
Artículo 142. El titular, por sí mismo o a través de su representante, podrá impugnar la resolución del recurso de revisión emitido por el Instituto ante el Instituto Nacional a través del recurso de inconformidad, según lo señalado en la Ley General, o bien impugnarse ante el Poder Judicial de la Federación a través del Juicio de Amparo.

Substanciación del Recurso de Inconformidad
Artículo 143. El recurso de Inconformidad se substanciará y resolverá en los términos establecidos por la Ley General y la Ley General de Transparencia y Acceso a la Información Pública.

Efectos del recurso de inconformidad en caso de modificación o revocación de la resolución del Instituto
Artículo 144. En los casos en que a través del recurso de inconformidad se modifique o revoque la resolución del Instituto, éste deberá emitir un nuevo fallo atendiendo los lineamientos que se fijaron al resolver la inconformidad, dentro del plazo de quince días, contados a partir del día siguiente al en que se hubiere notificado o se tenga conocimiento de la resolución dictada en la inconformidad.

Seguimiento y Vigilancia del debido cumplimiento por parte del Instituto
Artículo 145. Corresponderá al Instituto, en el ámbito de su competencia, realizar el seguimiento y vigilancia del debido cumplimiento por parte del responsable de la nueva resolución emitida como consecuencia de la inconformidad en términos de la presente Ley.

CAPÍTULO TERCERO

DE LA FACULTAD DE ATRACCIÓN DEL INSTITUTO NACIONAL

De la Facultad de Atracción
Artículo 146. El Pleno del Instituto, cuando así lo apruebe la mayoría de sus Comisionados, podrá formular petición fundada al Instituto Nacional, para que conozca de aquellos recursos de revisión pendientes de resolución en materia de datos personales, que por su interés y trascendencia así lo ameriten, en los plazos y términos previstos en la Ley General y demás normatividad aplicable.

TÍTULO DÉCIMO SEGUNDO
PROCEDIMIENTOS PARA VERIFICAR EL CUMPLIMIENTO DE LA LEY

CAPÍTULO ÚNICO
DE LAS FACULTADES DE VERIFICACIÓN

De las Facultades de Verificación y Vigilancia
Artículo 147. El Instituto tendrá la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta.

En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto estará obligado a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.

El responsable no podrá negar el acceso a la documentación solicitada con motivo de una verificación, o a sus sistemas o bases de datos personales, ni podrá invocar la reserva o la confidencialidad de la información.

Modalidades de inicio de las Verificaciones
Artículo 148. La verificación podrá iniciarse:

I. De oficio cuando el Instituto cuente con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes.

II. Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia.

El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma.

Cuando los hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado.

La verificación no procederá en los supuestos de procedencia del recurso de revisión o inconformidad previstos en la presente Ley.

La verificación no se admitirá en los supuestos de procedencia del recurso de revisión o inconformidad, previstos en la presente Ley.

Previo a la verificación respectiva, el Instituto podrá desarrollar investigaciones previas, con el fin de

contar con elementos para fundar y motivar el acuerdo de inicio respectivo.

Cuando derivado de la investigación de los casos de violación del derecho a la protección de datos personales, se desprenda que puede existir menoscabo de otros derechos humanos correlativos, el Instituto se coordinará con las instancias u organismos competentes, para la investigación correspondiente, con la finalidad de garantizar cabalmente la protección integral de dichos derechos humanos.

Atención de requerimientos por parte de autoridades
Artículo 149. Las autoridades del Estado deberán atender los requerimientos del Instituto, brindar auxilio y coadyuvar con las investigaciones, manteniendo confidencialidad de las actuaciones correspondientes.

Requisitos para la presentación de denuncias
Artículo 150. Para la presentación de una denuncia no podrán solicitarse mayores requisitos que los que se describen a continuación:

I. El nombre de la persona que denuncia, o en su caso, de su representante.

II. El domicilio ubicado en el Estado de México o medio para recibir notificaciones de la persona que denuncia.

III. La relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho.

IV. El responsable denunciado y su domicilio, o en su caso, los datos para su identificación y ubicación.

V. La firma del denunciante, o en su caso, de su representante. En caso de no saber firmar, bastará la huella digital.

La denuncia podrá presentarse por escrito libre, o a través de los formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto.

Una vez recibida la denuncia, el Instituto deberá acusar recibo de la misma. El acuerdo correspondiente se notificará al denunciante.

Requisitos aplicables a las Visitas de Verificación
Artículo 151. La verificación iniciará a través una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas los sistemas o las bases de datos personales respectivas.

Para la verificación en instancias de seguridad pública se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados, así como de una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines correspondientes.

El procedimiento de verificación deberá tener una duración máxima de cincuenta días.
El Instituto podrá ordenar medidas cautelares, si del desahogo de la verificación advierten un daño inminente o irreparable en materia de protección de datos personales, siempre y cuando no impidan el

cumplimiento de las funciones ni el aseguramiento de los sistemas o bases de datos de los sujetos obligados.

Estas medidas sólo podrán tener una finalidad correctiva y será temporal hasta entonces los sujetos obligados lleven a cabo las recomendaciones hechas por el Instituto.

La visita de verificación se entenderá iniciada a través de la notificación de la orden escrita, en la cual se indicarán los verificadores habilitados para el desarrollo de las diligencias.

La orden de verificación podrá incluir diversos sistemas y bases de datos personales pertenecientes al responsable.

Con la finalidad de dar inicio a los trabajos de verificación, los verificadores habilitados deberán llevar a cabo una reunión de apertura, en la cual explicarán a los administradores o personal sujetos a verificación, de manera general, el objeto y alcance del procedimiento.

Los verificadores habilitados para la visita deberán documentar sus actuaciones y diligencias a través de actas que deberán levantarse con la participación de dos testigos nombrados por el sujeto obligado, en caso que el sujeto obligado no designe a los testigos, éstos podrán ser designados por los verificadores.

En caso que las personas con las que se entiendan las diligencias, se nieguen a firmar las actas y demás documentación que se genere, bastará con que el o los verificadores habilitados asienten dicho hecho en el acta.

Una vez que los verificadores determinen que se ha cumplido con el objeto de la orden de verificación, deberán realizar el cierre de diligencias, acto en el cual podrán solicitar confirmación de evidencia a través de ratificaciones, copias certificadas o cualquier otro medio pertinente. En la misma diligencia deberán presentar sus apreciaciones preliminares acerca de los principales hallazgos detectados, a fin que el enlace que se designe en representación del sujeto obligado o los administradores sujetos a verificación, manifiesten lo que a su derecho convenga o exhiban pruebas en ese acto por comparecencia o por escrito, o dentro de los cinco días posteriores.

De la Conclusión del Procedimiento de Verificación
Artículo 152. El procedimiento de verificación concluirá con la resolución que emita el Instituto, en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.

Práctica de Auditorías Voluntarias
Artículo 153. Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.

TÍTULO DÉCIMO TERCERO
MEDIDAS DE APREMIO Y RESPONSABILIDADES

CAPÍTULO PRIMERO
DE LAS MEDIDAS DE APREMIO

Cumplimiento de las resoluciones del Instituto
Artículo 154. Para el cumplimiento de las resoluciones emitidas por el Instituto se deberá observar lo dispuesto en la Ley de Transparencia.

De las Medidas de Apremio
Artículo 155. El Instituto podrá imponer para asegurar el cumplimiento de sus determinaciones las medidas de apremio siguientes:

I. La amonestación pública.

II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y considerados en las evaluaciones que realicen éstos.

En caso que el incumplimiento de las determinaciones del Instituto implique la presunta comisión de un delito o una de las conductas señaladas en la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

Requerimiento a Superior Jerárquico
Artículo 156. Si a pesar de la ejecución de las medidas de apremio previstas en el artículo anterior no se cumpliere con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora.

De persistir el incumplimiento, se aplicarán sobre aquél las medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista a la autoridad competente en materia de responsabilidades.

Aplicación de las Medidas de Apremio
Artículo 157. Las medidas de apremio a que se refiere el presente Capítulo, deberán ser aplicadas por el Instituto, por sí mismo o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.

Medio para hacer efectivas las multas impuestas como medidas de apremio
Artículo 158. Las multas que fije el Instituto se harán efectivas por la Secretaría de Finanzas del Estado de México a través de los procedimientos que las leyes establezcan.

Calificación para la imposición de medidas de apremio
Artículo 159. Para calificar las medidas de apremio establecidas en el presente Capítulo, el Instituto deberá considerar:

I. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado, los indicios de intencionalidad, la duración del incumplimiento de las determinaciones del Instituto y la afectación al ejercicio de sus atribuciones.

II. La condición económica del infractor.

III. La reincidencia.

El Instituto establecerá a través de lineamientos de carácter general, las atribuciones de las áreas encargadas de calificar la gravedad de la falta de observancia a sus determinaciones y de la notificación y ejecución de las medidas de apremio que apliquen e implementen, conforme a los elementos desarrollados en este Capítulo.

Multa en caso de reincidencia
Artículo 160. En caso de reincidencia, el Instituto podrá imponer una multa equivalente hasta el doble de la que se hubiera determinado.

Se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.

Plazo para la aplicación e implementación de la medida de apremio
Artículo 161. Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir que sea notificada la medida de apremio al infractor.

Imposición de amonestación pública
Artículo 162. La amonestación pública será impuesta por el Instituto y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.

Disposiciones para la cuantificación de las medidas de apremio
Artículo 163. El Instituto podrá requerir al infractor la información necesaria para determinar su condición económica, apercibido que en caso de no proporcionar la misma, las multas se cuantificarán con base a los elementos que se tengan a disposición, tales como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de internet y en general cualquiera que evidencie su condición, quedando facultado el Instituto para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

Medio de impugnación en contra de las medidas de apremio
Artículo 164. En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante el Poder Judicial de la Federación.

CAPÍTULO SEGUNDO
DE LAS RESPONSABILIDADES

Supuestos de responsabilidad
Artículo 165. Serán causas de responsabilidad administrativa de las y los servidores públicos por incumplimiento de las obligaciones establecidas en la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales, así como los demás derechos previstos por esta Ley.

II. No contar con aviso de privacidad u omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere esta Ley.

III. No cumplir con las obligaciones relativas al aviso de privacidad.

IV. No inscribir los sistemas de datos personales en el registro en el plazo que previene esta Ley.

V. Declarar dolosamente la inexistencia de datos personales, cuando estos existan total o parcialmente en los archivos del sujeto obligado.

VI. Omitir reiteradamente dar respuesta a las solicitudes de acceso, rectificación, cancelación u oposición de datos personales dentro de los plazos previstos por esta Ley.

VII. Entregar intencionalmente de manera incompleta información requerida en una solicitud de datos personales.

VIII. Prolongar con dolo los plazos previstos para la respuesta de ejercicio de derechos ARCO o derechos relacionados en la materia.

IX. Incumplir el deber de confidencialidad establecido en esta Ley.

X. Recabar o transferir datos personales sin el consentimiento expreso del titular en los casos en que este sea exigible.

XI. Tratar datos personales cuando con ello se afecte el ejercicio de los derechos establecidos por la Constitución.

XII. Dar tratamiento a datos personales intencionalmente en contravención a los principios y deberes establecidos en esta Ley.

XIII. Mantener datos personales inexactos cuando resulte imputable a los sujetos obligados o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.

XIV. No cumplir con las medidas de seguridad que se determinen en esta Ley y en los lineamientos correspondientes.

XV. Crear sistemas de datos personales y bases de datos en contravención a lo dispuesto en esta Ley.

XVI. Obstruir actos de verificación, así como el ejercicio de las facultades del Instituto previstas en esta Ley.

XVII. Transferir datos personales, fuera de los casos previstos en esta Ley, cuando la misma haya tenido por objeto obtener un lucro indebido.

XVIII. No cesar en el uso ilícito de los tratamientos de datos personales cuando sea requerido para ello por el Instituto.

XIX. Usar, sustraer, destruir, mutilar, ocultar, inutilizar, divulgar o alterar total o parcialmente y de manera indebida, datos personales que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

XX. No acatar por dolo o negligencia las resoluciones emitidas por el Instituto.

XXI. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho que se trate.

XXII. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista

una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

XXIII. Presentar violaciones a la seguridad de los datos personales por la falta de implementación de medidas de seguridad que establece esta Ley.

XXIV. Omitir la entrega del informe anual y demás informes a que se refiere la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

XXV. Cualquier otro incumplimiento a las disposiciones establecidas en esta Ley.
Las responsabilidades a que se refiere este artículo o cualquier otra derivada del incumplimiento de las obligaciones establecidas en esta Ley serán fincadas a través de autoridad competente, previa promoción del fincamiento por parte del Instituto.

Las infracciones previstas en las fracciones XIV, XVI, XVII, XVIII, XIX, XX, XXI y XXIII o la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves para efectos de su sanción administrativa.

En caso que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y en su caso la sanción, corresponderán a la autoridad electoral competente.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Independencia de las Responsabilidades del orden Civil o Penal
Artículo 166. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo anterior, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables con independencia de las responsabilidades del orden civil o penal.

Incumplimiento por parte de Partidos Políticos
Artículo 167. Ante incumplimientos por parte de los partidos políticos, el Instituto dará vista al Instituto Electoral del Estado de México, para que resuelva lo conducente, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.

En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto deberá dar vista al órgano interno de control del sujeto obligado relacionado con éstos, cuando sean servidores públicos, con el fin que instrumenten los procedimientos administrativos a que haya lugar.

Promoción de Responsabilidades
Artículo 168. En aquellos casos en que el presunto infractor tenga la calidad de servidora o servidor público, el Instituto, deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un expediente en que se contengan todos los elementos que considere pertinentes para sustentar la presunta responsabilidad administrativa. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La autoridad que conozca del asunto, deberá informar de la conclusión del procedimiento y en su caso, de la ejecución de la sanción al Instituto.

A efecto de sustanciar el procedimiento citado en este artículo, el Instituto deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad.

Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba. La denuncia y el expediente deberán remitirse a la contraloría, órgano interno de control o equivalente dentro de los quince días siguientes a partir que el Instituto tenga conocimiento de los hechos.

Denuncia en caso de comisión de delitos
Artículo 169. En caso que el incumplimiento de las determinaciones del instituto implique la presunta comisión de un delito, deberá denunciar los hechos ante la autoridad competente.

TRANSITORIOS

PRIMERO. Publíquese el presente Decreto en el Periódico Oficial "Gaceta del Gobierno".

SEGUNDO. El presente Decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial "Gaceta del Gobierno".

TERCERO. La Ley de Protección de Datos Personales del Estado de México, publicada en el Periódico Oficial "Gaceta del Gobierno" el 31 de agosto de 2012, quedará abrogada con la entrada en vigor de la presente Ley.

CUARTO. Las solicitudes y recursos de revisión en trámite a la entrada en vigor de la Ley que se crea por este Decreto se resolverán conforme Ley vigente al momento de la presentación de la solicitud o interposición del recurso de revisión.

QUINTO. Los sujetos obligados deberán tramitar, expedir o modificar su normatividad interna a más tardar dentro de los doce meses siguientes a la entrada en vigor de esta Ley.

En el mismo plazo señalado en el párrafo anterior, los sujetos obligados deberán llevar a cabo la actualización del inventario y registro de sus sistemas y bases de datos personales en términos de esta Ley.

SEXTO. El Instituto contará con seis meses para armonizar su Programa de Cultura de la Transparencia y Protección de Datos Personales, a partir de la expedición del Programa Nacional. Las acciones que se desprendan deberán implementarse a más tardar en el ejercicio fiscal inmediato siguiente al en que fuera aprobada la armonización.

SÉPTIMO. El Instituto expedirá el Programa Estatal y Municipal de Protección de Datos Personales y lo publicará en el Periódico Oficial "Gaceta del Gobierno" a más tardar en un periodo de doce meses contados a partir de la entrada en vigor del presente Decreto.

OCTAVO. La Legislatura del Estado, deberá hacer las previsiones presupuestales necesarias para la operación de la presente Ley y establecer las partidas presupuestales específicas en el Presupuesto de Egresos del Estado para el Ejercicio Fiscal de 2018.

Para el caso de los municipios con una población menor a los setenta mil habitantes, el Instituto

instrumentará el Programa Juntos por la Protección de Datos Personales con el que de manera subsidiaria se fortalecerán las capacidades institucionales y la implementación de la presente Ley.

Sin perjuicio de lo anterior, la Secretaría de Finanzas, en un plazo máximo de treinta días naturales, contado a partir de la entrada en vigor de la presente Ley, proveerá con sujeción a las previsiones que para tal efecto estén contenidas en el Presupuesto de Egresos del Estado, los recursos adicionales necesarios al Instituto, para dar inicio a la implementación de las nuevas atribuciones contenidas en esta Ley.

NOVENO. La Secretaría de Finanzas realizará el estudio correspondiente a fin de proponer el esquema de ampliación presupuestal para la implementación por parte de sujetos obligados de las medidas de seguridad previstas en la presente Ley, en un plazo de ciento ochenta días posterior al inicio de su vigencia.

DÉCIMO. El Instituto deberá informar a la Legislatura, en el Informe Anual de Actividades, los avances en la implementación de los programas referidos en este Decreto.

DÉCIMO PRIMERO. El Código Financiero del Estado de México y Municipios deberá considerar en la determinación de los costos de reproducción y certificación para efectos de acceso a datos personales que los montos permitan o faciliten el ejercicio de este derecho.

Lo tendrá entendido el Gobernador del Estado, haciendo que se publique y se cumpla.

Dado en el Palacio del Poder Legislativo, en la ciudad de Toluca de Lerdo, capital del Estado de México, a los veintisiete días del mes de mayo del año dos mil diecisiete.- Presidente.- Dip. Aquiles Cortés López.- Secretarios.- Dip. María Mercedes Colín Guadarrama.- Dip. Areli Hernández Martínez.- Dip. Miguel Ángel Xolalpa Molina.-Rúbricas.

Por tanto, mando se publique, circule, observe y se le dé el debido cumplimiento.

Toluca de Lerdo, Méx., a 30 de mayo de 2017.

EL GOBERNADOR CONSTITUCIONAL
DEL ESTADO DE MÉXICO

DR. ERUVIEL ÁVILA VILLEGAS
(RÚBRICA).

EL SECRETARIO GENERAL DE GOBIERNO

JOSÉ S. MANZUR QUIROGA
(RÚBRICA).

APROBACIÓN: 27 de mayo de 2017.

PROMULGACIÓN: 30 de mayo de 2017.

PUBLICACIÓN: 30 de mayo de 2017.

VIGENCIA: El presente Decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial "Gaceta del Gobierno".