



Ciudad de México, a 19 de mayo de 2026

DIP. JESÚS SESMA SUÁREZ  
PRESIDENTE DE LA MESA DIRECTIVA DEL  
CONGRESO DE LA CIUDAD DE MÉXICO,  
III LEGISLATURA.  
P R E S E N T E.

El que suscribe Diputado **Andrés Atayde Rubiolo**, integrante del Grupo Parlamentario del Partido Acción Nacional en la III Legislatura del Congreso de la Ciudad de México, con fundamento en lo dispuesto en los artículos 71 fracción III y 122 apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos; 29 y 30, numeral 1, inciso b) de la Constitución Política de la Ciudad de México; 1, 4 fracción XXI 12 fracción II y 13 de la Ley Orgánica del Congreso de la Ciudad de México; 1,2 fracción XXI, 5 fracción I, 95 fracción II y 96 del Reglamento del Congreso de la Ciudad de México, someto a la consideración del pleno de este Asamblea la siguiente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO**, en los términos de la siguiente:

### EXPOSICIÓN DE MOTIVOS

#### I. Antecedentes normativos

La historia de la protección de datos personales en la Ciudad de México pasa por tres grandes etapas: la etapa preconstitucional local (Distrito Federal), la creación y maduración del marco normativo propio (LPDPDF/LPDPPSOCDMX) y la actual etapa de armonización con la Ley General y de reconfiguración institucional del sistema de transparencia.<sup>1</sup>

#### A. Primeros desarrollos normativos (DF y nivel federal)

En México, el derecho a la protección de datos personales comienza a consolidarse normativamente con la reforma constitucional de 2009 al artículo 6,

<sup>1</sup> [https://portal.infocdmx.org.mx/sites/default/files/biblioteca-digital/libro/El\\_derecho\\_de\\_proteccion\\_de\\_datos\\_personales\\_en\\_Mexico.pdf](https://portal.infocdmx.org.mx/sites/default/files/biblioteca-digital/libro/El_derecho_de_proteccion_de_datos_personales_en_Mexico.pdf)





que incorpora expresamente este derecho ligado al acceso a la información, y con la posterior reforma al artículo 16 que lo reconoce en el ámbito de particulares.<sup>2</sup>

Estos cambios federales abren el espacio para que el entonces Distrito Federal adopte su propia legislación en la materia y diseñe un órgano garante especializado, lo que convierte a la capital en uno de los primeros laboratorios normativos en protección de datos personales en el país.<sup>3</sup>

## **B. Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF)**

El punto de partida local es la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF), vigente antes de la transformación constitucional a Ciudad de México.<sup>4</sup>

Materiales de capacitación del propio Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF, extinto INFO CDMX) señalan que esta ley fue una de las primeras regulaciones locales específicas en materia de datos personales y que colocó al DF como referente nacional.<sup>5</sup>

## **C. Rol del InfoDF/INFO CDMX como órgano garante**

Desde su creación, el InfoDF asumió la doble función de órgano garante en acceso a la información y en protección de datos personales en el ámbito local, desarrollando criterios, lineamientos y una red de responsables de sistemas de datos en los sujetos obligados.<sup>6</sup>

En 2016, el propio Instituto destacó que la LPDPDF se había convertido en referente para la construcción de la futura norma general de protección de datos personales, subrayando que en la Ciudad *“existe un largo camino de trabajo sobre la protección de los datos personales en posesión de la autoridad”*.<sup>7</sup>

## **D. De Distrito Federal a Ciudad de México: nueva Constitución y Ley local**

<sup>2</sup> <https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/4.pdf>

<sup>3</sup> <https://infocdmx.org.mx/index.php/2-boletines/5330-dcs-148-16.html>

<sup>4</sup> <http://semujerestransparencia.cdmx.gob.mx/CAJ/PORTAL/NORMATIVIDAD/LPDPDF.pdf>

<sup>5</sup> <https://www.infocdmx.org.mx/capacitacion/publicacionesDCCT/manual5lpdpdf/manualdatospersonales.pdf>

<sup>6</sup> <https://www.revistaabogacia.com/info-cdmx-18-anos-como-organo-garante/>

<sup>7</sup> <https://infocdmx.org.mx/index.php/2-boletines/5330-dcs-148-16.html>





Con la expedición de la Constitución Política de la Ciudad de México y la transición formal del DF a Ciudad de México, fue necesario armonizar el marco local de protección de datos personales con la nueva configuración constitucional y con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.<sup>8</sup>

El 10 de abril de 2018 se publicó en la Gaceta Oficial de la Ciudad de México el decreto por el cual se expidió la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (LPDPPSOCDMX), que sustituyó a la LPDPDF y alineó el régimen local a los estándares de la Ley General.

### **E. Contenido y funcionamiento de la LPDPPSOCDMX**

La LPDPPSOCDMX se concibe como norma de orden público, de observancia general en toda la ciudad, que regula el tratamiento de datos personales por parte de autoridades de los poderes Ejecutivo, Legislativo y Judicial, alcaldías, organismos autónomos y demás sujetos obligados locales.<sup>9</sup>

Entre otros elementos, la ley recoge los principios y derechos ARCO/ARCOP/ARCOSP, establece obligaciones de seguridad administrativas, físicas y técnicas, prevé la figura del aviso de privacidad y regula el registro de sistemas de datos personales, que en la práctica se instrumenta mediante el Registro Electrónico de Sistemas de Datos Personales administrado por el INFO CDMX.

### **F. Desarrollo institucional reciente y consolidación del sistema local**

A lo largo de los años, INFO CDMX (antes InfoDF) ha consolidado su papel a través de lineamientos, manuales, cursos y redes de responsables de datos personales, lo que ha permitido construir un acervo de buenas prácticas y criterios en la protección de datos en la ciudad.<sup>10</sup>

Informes y notas institucionales dan cuenta de la actualización continua del padrón de sujetos obligados y del registro de sistemas de datos personales, reflejando la ampliación y sofisticación del sistema local de protección de datos en la CDMX.

<sup>8</sup> <https://www.ssc.cdmx.gob.mx/storage/app/media/Transparencia/Documentos%20Transparencia/guia-de-sistemas-de-datos-personales.pdf>

<sup>9</sup> <https://infocdmx.org.mx/index.php/normatividad-en-datos-personales>

<sup>10</sup> <https://infocdmx.org.mx/index.php/nuestras-actividades-y-servicios/biblioteca-digital/informes-de-actividades-y-resultados.html>





## 2. Evolución de la ley local en la CDMX (INFO CDMX)

El derecho a la protección de datos personales se construyó en México como un derecho humano autónomo y, al mismo tiempo, como límite al derecho de acceso a la información.<sup>11</sup>

En el plano federal, los antecedentes inmediatos están en las reformas al artículo 6 constitucional (derecho de acceso a la información y datos personales) y al artículo 16 (protección de datos personales), que dieron pie a la legislación general y local en la materia.<sup>12</sup>

El INFO CDMX reconoce como “principal instrumento normativo” en la Ciudad de México a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (LPDPPSOCDMX), de carácter de orden público e interés general.

El Instituto elaboró además normativa complementaria —Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados— y materiales de capacitación (curso “Introducción a la Ley de Protección de Datos Personales en posesión de sujetos obligados en la Ciudad de México”), cuyo Módulo 2 está dedicado específicamente a la “Evolución de la protección de datos personales en posesión de sujetos obligados en la Ciudad de México”.<sup>13</sup>

Un manual elaborado por INFO CDMX sobre la ley de datos personales para el entonces Distrito Federal incluye un “Módulo dos. Antecedentes de las leyes de protección de datos personales”, en el que se exponen las ideas básicas sobre la institucionalización del derecho y la cronología de la legislación mexicana y local.

## 3. Contenido y desarrollo de la LPDPPSOCDMX (normatividad INFO CDMX)

De acuerdo con las “Generalidades de la LPDPPSOCDMX” en el portal del INFO, la ley impone a los sujetos obligados la implementación de medidas de seguridad administrativas, físicas y técnicas para garantizar el tratamiento lícito de datos personales y la protección de los derechos ARCO.<sup>14</sup>

<sup>11</sup> <https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/10486/19730>

<sup>12</sup> <https://archivos.juridicas.unam.mx/www/bjv/libros/12/5669/4.pdf>

<sup>13</sup> <https://www.infocdmx.org.mx/cursodatospersonales/inicio/>

<sup>14</sup> <https://infocdmx.org.mx/index.php/normatividad-en-datos-personales>



La LPDPPSOCDMX se aplica a cualquier autoridad, órgano u organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos del gobierno de la Ciudad de México y partidos políticos locales, siempre que traten datos personales de personas físicas en el ejercicio de sus atribuciones.

El INFO CDMX ha actualizado el padrón de sujetos obligados en materia de transparencia y de protección de datos, lo que da cuenta de la extensión de la ley en el ámbito capitalino; por ejemplo, en 2024 se reporta que el padrón en materia de datos personales se integra por poco más de un centenar de instituciones obligadas.<sup>15</sup>

#### **4. Sistema nacional de transparencia y su impacto en la CDMX (Nexos)**

El ensayo “Un año después: el nuevo Sistema Nacional de Transparencia”, publicado en Nexos, analiza la reforma constitucional en materia de “simplificación orgánica” que eliminó organismos autónomos como el INAI y reconfiguró el Sistema Nacional de Transparencia.<sup>16</sup>

El texto detalla que la reforma supuso la sustitución del diseño original del Sistema Nacional de Transparencia y de los órganos garantes autónomos por un modelo fragmentado de autoridades administrativas en cada poder y ámbito, lo que impacta el modo en que se garantiza el acceso a la información y la protección de datos personales tanto a nivel federal como local.<sup>17</sup>

#### **5. Reconfiguración institucional y nuevos órganos garantes**

A partir de la nueva Ley General de Transparencia y de la reforma que elimina al INAI, se crea un nuevo modelo en el que funciones antes concentradas en un órgano constitucional autónomo se reparten entre múltiples autoridades de transparencia y de protección de datos por poder y por ámbito.<sup>18</sup>

En el plano federal, la reforma implica la desaparición de la Ley Federal de Transparencia y la modificación de las leyes generales y federales de protección de

<sup>15</sup> <https://infocdmx.org.mx/index.php/normatividad-en-datos-personales>

<sup>16</sup> <https://anticorrupcion.nexos.com.mx/un-ano-despues-el-nuevo-sistema-nacional-de-transparencia/>

<sup>17</sup> <https://www.gilysolis.com.mx/post/adi%C3%B3s-al-inai-qu%C3%A9-significa-la-nueva-ley-de-transparencia-en-m%C3%A9xico>

<sup>18</sup> <https://transparencia.gob.mx/home.html>





datos en posesión de sujetos obligados y de particulares; en lo local, cada entidad federativa —incluida la Ciudad de México— debe armonizar su propia ley de protección de datos personales para ajustarse al nuevo arreglo institucional<sup>19</sup>

## II. PLANTEAMIENTO DEL PROBLEMA

La presente iniciativa tiene por objeto expedir una nueva Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, en armonización con la reforma constitucional federal publicada en el Diario Oficial de la Federación el 20 de marzo de 2025, así como con la reforma a la Constitución Política de la Ciudad de México publicada en la Gaceta Oficial de la Ciudad de México en diciembre de 2025, por la cual se rediseñó el modelo institucional para la garantía del derecho a la protección de datos personales en el ámbito local.

La reforma al artículo 6° apartado A y al artículo 134 de la Constitución Política de los Estados Unidos Mexicanos suprimió el carácter de órganos constitucionales autónomos a los organismos garantes en materia de transparencia, acceso a la información y protección de datos personales, y trasladó sus atribuciones a estructuras administrativas dentro del Poder Ejecutivo, bajo principios de austeridad republicana, eficiencia presupuestal y racionalidad institucional, sin que ello implique menoscabo en la tutela efectiva de los derechos.

En consecuencia, el Constituyente Permanente de la Ciudad de México aprobó la reforma al artículo 7, apartado E, numeral 5, y a los preceptos correlativos de la Constitución Política de la Ciudad de México, transfiriendo las funciones del extinto Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX) a un órgano desconcentrado de la Secretaría de la Contraloría General de la Ciudad de México, así como a las unidades de transparencia y autoridades garantes de los demás Poderes y órganos constitucionales autónomos, con el objeto de asegurar que la protección del derecho fundamental persista bajo un esquema institucional renovado.

Esta nueva arquitectura institucional exige que el marco legislativo local de protección de datos personales sea integralmente reformulado, no únicamente para sustituir referencias al organismo garante extinto, sino para incorporar las mejores prácticas legislativas en materia de derechos ARCO (acceso, rectificación,

<sup>19</sup> <https://www.gilysolis.com.mx/post/adi%C3%B3s-al-inai-qu%C3%A9-significa-la-nueva-ley-de-transparencia-en-m%C3%A9xico>



cancelación y oposición), evaluación de impacto en la protección de datos personales, encargados, cómputo en la nube, transferencias internacionales, principios de portabilidad y un régimen sancionatorio armonizado y técnicamente robusto.

## II. ARGUMENTOS QUE LA SUSTENTAN Y FUNDAMENTOS LEGALES

El 15 de diciembre de 2025, el Congreso de la Ciudad de México aprobó, mediante votación nominal con 45 votos a favor, el dictamen de la reforma constitucional en materia de transparencia, acceso a la información pública y protección de datos personales, publicado en la Gaceta Oficial de la Ciudad de México el 19 de diciembre de 2025.<sup>20</sup>

Dicha reforma modifica la Constitución Política de la Ciudad de México de la siguiente manera:

- **Adiciona** el numeral 5 al Apartado E del Artículo 7.º, estableciendo que la defensa y garantía del derecho de acceso a la información pública, la privacidad y la protección de datos personales en posesión de sujetos obligados estará a cargo de la Secretaría de la Contraloría General, a través del órgano desconcentrado que para tal efecto prevea la ley secundaria en la materia, así como de las autoridades garantes que corresponda.
- **Deroga** el inciso d) del Apartado A del Artículo 46, que reconocía al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, como organismo constitucional autónomo.
- **Deroga** el Artículo 49 de la Constitución local.
- **Reforma** el numeral 2 del Artículo 63, adecuando la integración del Comité Coordinador del Sistema Anticorrupción de la Ciudad de México.

Los artículos transitorios del decreto constitucional establecen que sus efectos materiales quedarán sujetos a la expedición de la legislación secundaria correspondiente, para la cual el Congreso de la Ciudad de México dispone de un **plazo máximo de 180 días naturales**, contados a partir del día siguiente a la

<sup>20</sup> [https://data.consejeria.cdmx.gob.mx/portal\\_old/uploads/gacetas/bbd22f0b2fab730aa4dc56e3e207b4c1.pdf](https://data.consejeria.cdmx.gob.mx/portal_old/uploads/gacetas/bbd22f0b2fab730aa4dc56e3e207b4c1.pdf)



publicación en la Gaceta Oficial, es decir, a partir del 20 de diciembre de 2025, por lo que dicho plazo vence el 18 de junio de 2026.

## Nuevo modelo institucional de la Ciudad de México

En congruencia con el mandato constitucional, el nuevo modelo institucional de transparencia de la Ciudad de México contempla la existencia de **once órganos garantes** distribuidos de la siguiente manera:

1. Un **órgano administrativo desconcentrado** sectorizado a la Secretaría de la Contraloría General, que abarcará al Poder Ejecutivo y a las 16 demarcaciones territoriales.
2. Una **Autoridad garante** adscrita al Poder Legislativo.
3. Una **Autoridad garante** adscrita al Poder Judicial.
4. Ocho **Autoridades garantes internas** en los organismos autónomos: Fiscalía General de Justicia, Instituto Electoral de la Ciudad de México, Comisión de Derechos Humanos de la Ciudad de México, Universidad Autónoma de la Ciudad de México, entre otros.

Este nuevo diseño replica el modelo adoptado a nivel federal, donde la Secretaría Anticorrupción y Buen Gobierno asumió las funciones del extinto INAI a través del órgano desconcentrado denominado "Transparencia para el Pueblo".

Entre los rasgos distintivos de la iniciativa se encuentran:

I) la definición renovada de las Autoridades Garantes en el ámbito local, integradas por el órgano desconcentrado de la Secretaría de la Contraloría General de la Ciudad de México y por los órganos internos de control u órganos especializados de los Poderes Legislativo, Judicial y de los órganos constitucionales autónomos;

II) el reconocimiento expreso de las alcaldías como sujetos obligados en su carácter de órganos político-administrativos de las demarcaciones territoriales;

III) la incorporación de un capítulo de evaluación de impacto en la protección de datos personales adaptado a la realidad operativa de la Administración Pública de la Ciudad de México;

IV) la armonización del régimen de transferencias con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y

V) un régimen integrado de medidas de apremio y sanciones con criterios de proporcionalidad y debido proceso.

Es así, que también se desea destacar este apartado de la Ley:





## Protección de Datos Personales y la tensión al derecho a la verdad en el Contexto de Desapariciones

México enfrenta una crisis de desapariciones de dimensiones estructurales que interpela directamente el alcance y los límites del derecho a la protección de datos personales en posesión de sujetos obligados.

De acuerdo con el Registro Nacional de Personas Desaparecidas y No Localizadas (RNPDNO), entre el 31 de diciembre de 1952 y el 18 de diciembre de 2025 se acumula un registro de **387,319 personas desaparecidas, no localizadas o localizadas**, de las cuales **133,520 —34.47% del total— permanecen desaparecidas o no localizadas** a la fecha del último corte disponible.

La Ciudad de México figura como la entidad federativa con mayor número de desapariciones en los primeros seis meses de 2025: **1,099 personas desaparecidas o no localizadas**, un incremento del **88% respecto al mismo periodo de 2024**, cuando se reportaron 585 casos; las alcaldías con mayor incidencia son Iztapalapa (227 casos), Cuauhtémoc (140) y Gustavo A. Madero (132).

Esta realidad coloca a los sujetos obligados de la Ciudad de México —en particular la Fiscalía de Justicia, las alcaldías, la Secretaría de Seguridad Ciudadana y la Comisión de Búsqueda de Personas— ante la obligación de gestionar bases de datos de personas desaparecidas que contienen datos personales de las víctimas directas, sus familiares, testigos y personal forense, cuya inadecuada protección puede amplificar los riesgos de revictimización, estigmatización y obstaculización de las investigaciones.

Ante este escenario, el marco normativo impone una obligación constitucional de doble naturaleza que la presente iniciativa debe reconocer explícitamente: por un lado, el deber de proteger la privacidad y los datos personales de las víctimas y sus familias —cuya divulgación indebida puede derivar en su victimización secundaria—; por otro, la obligación de garantizar el **derecho a la verdad**, que la Primera Sala de la Suprema Corte de Justicia de la Nación definió con claridad en el amparo en revisión **1077/2019** (Ministro Ponente: Alfredo Gutiérrez Ortiz Mena, resuelto por unanimidad el 16 de junio de 2021):

*"no bastará con obtener cualquier respuesta del sistema jurídico, sino que — en el caso particular de la desaparición forzada— es necesario que esa respuesta*





sea el producto de una investigación exhaustiva e imparcial, conducida a partir de la presunción de vida de la persona desaparecida, empeñada y comprometida con su hallazgo y en la persecución penal de los responsables".

En el mismo precedente, la Corte sostuvo que *"los errores, descuidos, dilaciones injustificadas de estas investigaciones conllevan violaciones al derecho a la verdad e impiden el acceso a la justicia"*, lo que traduce en una obligación de máxima diligencia en el tratamiento de la información vinculada a personas desaparecidas.

Esta tensión entre privacidad y verdad se resuelve en el plano normativo con una regla general que la presente iniciativa asume expresamente: **la información relacionada con violaciones graves a derechos humanos o delitos de lesa humanidad no puede clasificarse como reservada ni invocarse la protección de datos personales para negar el acceso de las familias a los expedientes o carpetas de investigación.**

La SCJN ya estableció este criterio al resolver que, en casos vinculados a crímenes de lesa humanidad —categoría en la que puede encuadrarse la desaparición forzada sistemática, según el artículo 5 de la Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas y el artículo 7.2.i del Estatuto de Roma—, el principio de máxima publicidad prevalece sobre la reserva y la confidencialidad de datos personales de terceros involucrados (*Tesis: DELITOS O CRÍMENES DE LESA HUMANIDAD. SU CONCEPTO PARA EFECTOS DEL DERECHO DE ACCESO A LA INFORMACIÓN DE LA AVERIGUACIÓN PREVIA QUE LOS INVESTIGA*, Registro 2000209, Semanario Judicial de la Federación, Décima Época).

En el plano legislativo, la Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas (publicada en el DOF el 17 de noviembre de 2017, con última reforma al 1° de abril de 2024) establece en su artículo 116 que *"la información contenida en el Registro Nacional de Personas Fallecidas y No Identificadas estará sujeta a las disposiciones en materia de protección de datos personales y se utilizará únicamente para lograr la identificación de las personas fallecidas"*.

Esta regla especial evidencia que el legislador federal ya reconoció la necesaria articulación entre el régimen de datos personales y los registros de





búsqueda, pero lo hizo de manera sectorial y sin que existan hoy, en el ámbito de la Ciudad de México, disposiciones locales que especifiquen cómo deben conciliar los sujetos obligados locales sus obligaciones en materia de protección de datos con el deber de acceso de las familias a la información sobre personas desaparecidas.

Asimismo, el Protocolo Homologado para la Búsqueda de Personas Desaparecidas y No Localizadas —actualizado por el Sistema Nacional de Búsqueda en su segunda sesión ordinaria del 15 de diciembre de 2025 y publicado en el DOF el 24 de marzo de 2026— dispone expresamente que *"las bases de datos y registros de personas desaparecidas deben respetar la voluntad e intimidad de las personas desaparecidas y sus familiares"*, reforzando la necesidad de un marco local armonizado.

La presente iniciativa atiende esta laguna normativa al establecer que los sujetos obligados de la Ciudad de México, cuando traten datos personales en el contexto de investigaciones sobre desapariciones, deben observar simultáneamente:

- i) el principio de finalidad específica previsto en el artículo 17 de esta Ley, que limita el uso de la información al objeto concreto de búsqueda e identificación;
- ii) la obligación de garantizar el acceso preferente de las víctimas indirectas —familiares— al expediente o carpeta de investigación, en los términos del amparo en revisión 1077/2019; y
- iii) la prohibición absoluta de clasificar como reservados o confidenciales los datos personales contenidos en registros de búsqueda cuando dicha clasificación tenga por efecto impedir el ejercicio del derecho a la verdad. Lo anterior no supone una excepción al régimen general de protección de datos: supone su aplicación integral y diferenciada, fundada en los principios de proporcionalidad, progresividad y pro persona que articulan la presente Ley con el bloque de constitucionalidad en materia de derechos humanos.

El presente diseño institucional, si bien sustituye un órgano constitucional autónomo por autoridades administrativas especializadas, incorpora las siguientes salvaguardas que garantizan la no regresividad en la tutela efectiva del derecho a la protección de datos personales:

1. **Independencia técnica y funcional** en el ejercicio de atribuciones especializadas;
2. **Profesionalización y estabilidad** del personal especializado.



3. **Prohibición expresa de interferencia** política o jerárquica;
4. **Control judicial pleno** de todas las resoluciones administrativas;
5. **Transparencia y rendición de cuentas** mediante publicación de resoluciones y criterios;
6. **Coordinación nacional** a través del Sistema Nacional de Transparencia;
7. **Sanciones efectivas** para garantizar cumplimiento;
8. **Evaluación continua** del impacto institucional.

El diseño propuesto responde al mandato constitucional de armonización con la reforma federal de 2025, pero preserva y, en ciertos aspectos, **fortalece** los mecanismos sustantivos y procedimentales de protección mediante

### Estándares internacionales.

La iniciativa incorpora varios estándares internacionales en materia de protección de datos, aunque la mayoría se reflejan de forma material (principios y figuras) más que por citas expresas a instrumentos concretos.

ESTÁNDAR INTERNACIONAL	CÓMO SE REFLEJA EN LA INICIATIVA
Bloque de convencionalidad en DDHH (instrumentos internacionales ratificados)	Art. 8: ordena interpretar la ley conforme a la Constitución federal, la Constitución de la CDMX, la Ley General y “los instrumentos jurídicos internacionales ratificados por nuestro país”, insertando la norma en el bloque de convencionalidad.
Enfoque de dignidad, libre desarrollo y autodeterminación informativa	Exposición de motivos: vincula el derecho a la protección de datos con la autodeterminación informativa, la dignidad humana y el libre desarrollo de la personalidad, como lo hacen el Convenio 108/108+ y la doctrina europea e interamericana. <sup>21</sup>
Derecho humano autónomo y límite al acceso a la información	Se explica la evolución del derecho en México como derecho humano autónomo y como límite al acceso a la información, alineado con el enfoque de derechos de privacidad en el Convenio 108.

### Principios del RGPD y del Convenio 108/108+

<sup>21</sup> <https://basham.com.mx/entra-en-vigor-tratado-internacional-de-proteccion-de-datos/>



PRINCIPIO RGPD / CONVENIO 108	CÓMO APARECE EN LA INICIATIVA CDMX
Licitud, lealtad y transparencia	Art. 17 obliga a los sujetos obligados a observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento.
Limitación de la finalidad	Art. 20 exige que solo se traten datos adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento, conectando finalidad y proporcionalidad.
Minimización de datos (proporcionalidad)	Art. 20 recoge expresamente el principio de proporcionalidad: tratamiento solo de datos adecuados, relevantes y estrictamente necesarios, lo que replica la “minimización de datos” del RGPD. <sup>22</sup>
Exactitud de los datos	Art. 18 obliga a adoptar medidas para mantener los datos exactos, completos, correctos y actualizados, e incluso presume calidad cuando los proporciona directamente la persona titular.
Limitación del plazo de conservación	Art. 18 y 19 regulan plazos de conservación: no deben exceder lo necesario para la finalidad, con obligación de bloqueo y posterior supresión, en línea con la limitación de almacenamiento del RGPD. <sup>23</sup>
Integridad y confidencialidad (seguridad)	Arts. 92–99 establecen medidas de seguridad administrativas, técnicas y físicas basadas en análisis de riesgo, sensibilidad de datos y tratamientos, con deber de prevenir accesos no autorizados, daños o pérdidas.
Responsabilidad proactiva (accountability)	Art. 17 incorpora el principio de responsabilidad y el art. 23 obliga a establecer políticas, programas, auditorías, capacitación y sistemas de supervisión para acreditar cumplimiento, reflejando la lógica de accountability del RGPD.
Protección de datos desde el diseño y por defecto	Arts. 23, 27 y 36–37 exigen diseñar políticas, programas, sistemas, plataformas y tecnologías que cumplan por defecto con la Ley, lo que reproduce el estándar de “data protection by design and by default”.

## Derechos de las personas titulares

<sup>22</sup> <https://www.iubenda.com/es/blog/cuales-son-los-7-principios-del-rgpd/>

<sup>23</sup> <https://basham.com.mx/entra-en-vigor-tratado-internacional-de-proteccion-de-datos/>



ESTÁNDAR INTERNACIONAL	CONTENIDO	REFLEJO EN LA INICIATIVA
Derecho de acceso	Todo titular debe poder conocer qué datos se tratan y cómo, con medios efectivos.	Art. 11 reconoce el derecho de acceso a los datos en posesión del sujeto obligado y a conocer condiciones y generalidades del tratamiento, con procedimientos sencillos y gratuitos.
Derechos de rectificación, cancelación y oposición	Posibilidad efectiva de corregir, borrar u oponerse a tratamientos que afecten derechos o sean incompatibles con la finalidad.edpb.europa	Arts. 12–14 desarrollan rectificación, cancelación y oposición, incluyendo supresión como fase ejecutiva de la cancelación y la posibilidad de limitar el tratamiento mientras se resuelve una controversia.
Recursos efectivos y tutela por autoridad independiente/especializada	Estándares de sistemas europeo e interamericano: derecho a un recurso efectivo ante autoridad con facultades para investigar, ordenar y sancionar.	Títulos sobre autoridades garantes y procedimientos de verificación y recursos de revisión (no íntegros en los fragmentos, pero referidos en la exposición de motivos) contemplan facultades de verificación, medidas cautelares, sanciones y medios de impugnación.

### Datos sensibles y grupos protegidos

ESTÁNDAR INTERNACIONAL	CÓMO SE CUMPLE EN LA INICIATIVA
Protección reforzada para datos sensibles (salud, origen étnico, creencias, orientación sexual, etc.) como exige el RGPD y el Convenio 108	Art. 3, fracc. XII, define datos personales sensibles con lista casi idéntica a la del estándar internacional; art. 7 prohíbe su tratamiento salvo consentimiento expreso o supuestos tasados.





ESTÁNDAR INTERNACIONAL	CÓMO SE CUMPLE EN LA INICIATIVA
Protección especial de niñas, niños y adolescentes (Convención sobre los Derechos del Niño, estándares del Comité de Derechos del Niño)	Art. 7 obliga a privilegiar el interés superior de la niñez en el tratamiento de datos de niñas, niños y adolescentes, con obligaciones reforzadas para sujetos obligados.

### Evaluaciones de impacto y gestión de riesgo

ESTÁNDAR INTERNACIONAL	CÓMO SE REFLEJA
Evaluación de impacto en protección de datos (Data Protection Impact Assessment, DPIA) del RGPD	Art. 3, fracc. XVII, define la evaluación de impacto y la iniciativa incorpora un capítulo específico para tratamientos intensivos o relevantes, con obligación de identificar y mitigar riesgos.
Gestión de riesgos y seguridad basada en análisis de riesgo (buenas prácticas OCDE, ISO y RGPD)	Definición de análisis de riesgo y análisis de brecha (art. 3, fraccs. I y II), obligación de sistemas de gestión y documentación de medidas de seguridad (arts. 92–99), alineados con estándares de seguridad de la información.

### Transferencias internacionales y flujos transfronterizos

ESTÁNDAR INTERNACIONAL	CONTENIDO	CÓMO SE INCORPORA
Convenio 108 y Protocolo Adicional: flujos transfronterizos con garantías adecuadas y cooperación entre autoridades	El Convenio 108 compromete a facilitar el flujo de datos entre Estados miembros y asegurar protección adecuada frente a terceros Estados.	La iniciativa, siguiendo la Ley General, regula transferencias internacionales exigiendo obligaciones equivalentes del receptor, instrumentos jurídicos que detallan finalidades y medidas de protección, y respeto a tratados suscritos por México.
RGPD: transferencias	Exige “garantías adecuadas” para el	La iniciativa prevé que las transferencias se documenten mediante contratos o





ESTÁNDAR INTERNACIONAL	CONTENIDO	CÓMO SE INCORPORA
solo a países con nivel adecuado o con garantías apropiadas (cláusulas contractuales, etc.)	receptor y mecanismos contractuales o normativos.	convenios y que el tercero receptor trate los datos conforme a los principios y deberes de la ley y la Ley General, replicando la lógica de garantías apropiadas.

### Seguridad, vulneraciones y notificación

ESTÁNDAR INTERNACIONAL	CÓMO SE REFLEJA
Medidas de seguridad apropiadas al riesgo: técnicas y organizativas (RGPD, Convenio 108)	Arts. 25, 92–99 distinguen medidas de seguridad administrativas, técnicas y físicas, basadas en el tipo de datos, riesgos, número de titulares y antecedentes de incidentes; se exige documento de seguridad y sistema de gestión. <sup>24</sup>
Notificación de brechas de seguridad	El RGPD exige informar a autoridades y titulares cuando la violación de seguridad suponga alto riesgo.

### Supervisión, sanciones y recursos

ESTÁNDAR INTERNACIONAL	CÓMO SE CUMPLE
Autoridades de control con facultades de supervisión, investigación y sanción (RGPD, Convenio 108)	Aunque se sustituye el órgano autónomo, la iniciativa configura autoridades garantes administrativas con facultades de verificación, medidas de apremio, imposición de sanciones, emisión de lineamientos y atracción de casos relevantes.

<sup>24</sup> <https://www.iubenda.com/es/blog/cuales-son-los-7-principios-del-rgpd/>



ESTÁNDAR INTERNACIONAL	CÓMO SE CUMPLE
Recursos efectivos y debido proceso	Los procedimientos contemplan plazos claros, derecho de audiencia, motivación de resoluciones, recursos de revisión y posibles medios adicionales según la Ley de Procedimiento Administrativo, cumpliendo el estándar de debido proceso.

**FUNDAMENTOS LEGALES QUE LA SUSTENTAN**

ORDEN JURIDICO	REFERENCIA NORMATIVA	CONTENIDO O FUNCIÓN PRINCIPAL
1. Constitución federal	CPEUM, art. 6, apartado A	Reconoce el derecho de acceso a la información y la protección de datos personales frente a sujetos obligados.
1. Constitución federal	CPEUM, art. 16, párr. segundo	Reconoce el derecho a la protección de datos personales (acceso, rectificación, cancelación y oposición) y fija límites al tratamiento.
1. Constitución federal	CPEUM, art. 122, apdo. A, fracc. II	Define el régimen jurídico de la Ciudad de México y las facultades de su Congreso.
1. Constitución federal	CPEUM, art. 134	Establece principios de eficiencia, economía, transparencia y honradez en uso de recursos públicos.
2. Tratados	Convención Americana sobre Derechos Humanos, art. 11	Protege la honra y la vida privada; soporte convencional del derecho a la privacidad.
2. Tratados	PIDCP, art. 17	Prohíbe injerencias arbitrarias o ilegales en la vida privada y los datos personales.
2. Tratados	Convenio 108 del Consejo de Europa y Protocolo Adicional	Estándar técnico en tratamiento de datos y flujos transfronterizos, tomado como referencia.





ORDEN JURIDICO	REFERENCIA NORMATIVA	CONTENIDO O FUNCIÓN PRINCIPAL
3. Leyes generales	LGPDPPO, arts. 1–4	Objeto, ámbito de aplicación, definiciones y principios de protección de datos personales.
3. Leyes generales	LGPDPPO, arts. 6–8	Desarrollan principios, deber de seguridad y derechos ARCO; base de los artículos sustantivos de la iniciativa.
3. Leyes generales	LGTAIP, art. 44 y correlativos	Regulan la Plataforma Nacional de Transparencia y el Sistema Nacional de Transparencia.
4. Leyes federales	LFPDPPP, arts. 1–3	Referente técnico para el régimen de datos en posesión de particulares.
5. Constitución local	Constitución de la CDMX, art. 7, apdo. E, nums. 1, 4 y 5	Reconoce el derecho a la protección de datos, la portabilidad y el diseño institucional local.
6. Leyes locales generales	LPDPPSOCDMX vigente (ley actual)	Régimen local de datos personales en sujetos obligados que se pretende abrogar y sustituir.
6. Leyes locales generales	Ley de Transparencia de la CDMX	Regula sujetos obligados, Comité de Transparencia y Unidad de Transparencia.
6. Leyes locales generales	Ley Orgánica del Congreso de la CDMX, arts. 1, 4 fr. XXI, 12 fr. II, 13	Fundamenta competencia del Congreso y de las y los diputados para presentar la iniciativa.
6. Leyes locales generales	Reglamento del Congreso de la CDMX, arts. 1, 2 fr. XXI, 5 fr. I, 95 fr. II, 96	Regula el procedimiento parlamentario de presentación y trámite de iniciativas.
7. Leyes sectoriales locales	Ley de Procedimiento Administrativo de la CDMX	Norma supletoria para los procedimientos administrativos previstos en la iniciativa.





ORDEN JURIDICO	REFERENCIA NORMATIVA	CONTENIDO O FUNCIÓN PRINCIPAL
7. Leyes sectoriales locales	Ley para la Localización, Recuperación e Identificación Forense de Personas de la CDMX	Marco específico para el tratamiento de datos en sistemas de información de personas desaparecidas y fallecidas.
8. Lineamientos nacionales	Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados del SNT	Desarrollo técnico de la LGPDPPSO: medidas de seguridad, avisos de privacidad, procedimientos.
8. Lineamientos nacionales	Criterios del Sistema Nacional de Transparencia	Criterios para tratamientos intensivos o relevantes y para la portabilidad de datos personales.
9. Legislación comparada	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila (27-06-2025)	Referencia técnica integral para la estructura y contenido de la iniciativa de la CDMX.

**IV. PROBLAMETICA DESDE LA PERSPECTIVA DE GÉNERO, EN SU CASO.**

No aplica.

**V. ORDENAMIENTOS A MODIFICAR.**

La iniciativa se estructura en seis títulos que van de reglas generales a procedimientos y sanciones.

**VI. IMPACTO PRESUPUESTAL**

No aplica

**VII. TEXTO NORMATIVO PROPUESTO.**

La iniciativa se estructura en seis títulos que van de reglas generales a procedimientos y sanciones. Te dejo un resumen muy sintético por título, útil para dictamen o ficha.



## **Título Primero. Disposiciones generales**

Define objeto, ámbito de aplicación y principios de la ley (licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad). Regula conceptos básicos como datos personales, datos sensibles, aviso de privacidad, tratamiento, fuentes de acceso público, sistema de gestión y evaluación de impacto.

Determina quiénes son sujetos obligados, la relación con personas encargadas y proveedores (incluido cómputo en la nube), el Comité de Transparencia, la Unidad de Transparencia, las Autoridades Garantes y su coordinación con el Sistema Nacional y el Sistema Local de Transparencia.

## **Título Segundo. Derechos de las personas titulares y su ejercicio**

Reconoce los derechos ARCO (acceso, rectificación, cancelación, oposición) como núcleo del derecho a la protección de datos personales.

Fija reglas para su ejercicio: gratuidad, plazos de respuesta, requisitos mínimos de la solicitud, causales de improcedencia, límites al tratamiento y protección reforzada para niñas, niños, adolescentes, personas con discapacidad y personas fallecidas.

## **Título Tercero. Autoridades responsables y sujetos obligados**

Precisa quiénes son sujetos obligados (poderes Ejecutivo, Legislativo y Judicial, alcaldías y organismos autónomos), sus obligaciones de calidad, proporcionalidad y seguridad en el tratamiento y conservación de datos.

Regula la organización interna: funciones del Comité de Transparencia como máxima autoridad en datos personales en cada sujeto obligado, atribuciones de la Unidad de Transparencia y posibles oficiales de protección de datos.

## **Título Cuarto. Procedimientos administrativos en materia de datos personales**

Regula el procedimiento para ejercer los derechos ARCO: presentación de solicitudes, prevención, admisión, respuesta, plazos y modalidades de acceso, así como el tratamiento posterior a la respuesta.

Incluye reglas sobre tratamiento de datos (finalidades, consentimiento y sus excepciones), avisos de privacidad simplificado e integral, portabilidad,





transferencias y remisiones nacionales e internacionales, medidas de seguridad, gestión de incidentes y notificación de vulneraciones.

### **Título Quinto. Medios de impugnación**

Establece el recurso de revisión ante las Autoridades Garantes cuando se niegue o restrinja indebidamente el ejercicio de derechos ARCO o se incumplan obligaciones en materia de datos personales.

Regula el procedimiento de verificación de oficio o a instancia de parte, las pruebas admisibles, las resoluciones (vinculantes, definitivas e inatacables para los sujetos obligados) y sus efectos.

### **Título Sexto. Medidas de apremio, infracciones y sanciones**

Prevé medidas de apremio (amonestación pública y multa) para hacer cumplir las determinaciones de las Autoridades Garantes, así como criterios para graduarlas.

Tipifica infracciones administrativas de los sujetos obligados y personas servidoras públicas (por ejemplo, uso indebido de datos, falta de aviso de privacidad, ausencia de medidas de seguridad, transferencias ilegales), y establece sanciones que van de la suspensión a la destitución e inhabilitación, sin perjuicio de responsabilidades civiles o penales.

La iniciativa que se somete a esta Soberanía cumple, además, con los principios constitucionales de progresividad, pro persona y no regresión en materia de derechos humanos, al preservar y, en su caso, fortalecer las garantías procedimentales y sustantivas previstas en la legislación vigente, sin merma alguna del nivel de protección reconocido hasta la fecha a las personas titulares de los datos.

En atención a lo expuesto, y considerando la trascendencia del derecho fundamental a la protección de datos personales como pilar de la autodeterminación informativa, la dignidad humana y el libre desarrollo de la personalidad en el marco de la sociedad de la información, se propone a esta Soberanía la siguiente:

## **VIII. D E C R E T O**

**ARTÍCULO ÚNICO.-** Se expide la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, para quedar como sigue:



III LEGISLATURA



III LEGISLATURA



## LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO

### TÍTULO PRIMERO DISPOSICIONES GENERALES CAPÍTULO ÚNICO DISPOSICIONES PRELIMINARES

**Artículo 1.** La presente Ley es de orden público, de observancia general en toda la Ciudad de México y tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de Sujetos obligados, en términos de los artículos 6, Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, y el artículo 7 de la Constitución Política de la Ciudad de México.

Las disposiciones de esta Ley son de aplicación y observancia directa para los Sujetos obligados de la Ciudad de México, en el ámbito de su competencia.

Las Autoridades Garantes ejercerán las atribuciones y facultades que les otorgan la presente Ley, la Ley General y demás disposiciones aplicables, con independencia técnica en sus resoluciones y conforme exclusivamente a criterios jurídicos especializados.

**Artículo 2.** Son objetivos de esta Ley:

I. Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;

II. Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;

III. Proteger los datos personales en posesión de los Sujetos obligados por esta Ley, con la finalidad de regular su debido tratamiento;

IV. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;

V. Promover, fomentar y difundir una cultura de protección de datos personales;

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

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





I. Análisis de brecha: Herramienta de análisis para comparar el estado y desempeño real de los Sujetos obligados, en relación a las medidas de seguridad existentes, a partir de puntos de referencia seleccionados en una situación o momento dado, respecto a las faltantes en materia de protección de datos personales;

II. Análisis de riesgo: Estudio de las causas de las posibles amenazas, vulnerabilidades y probables eventos no deseados que puedan producir daños y perjuicios a la protección de datos personales;

III. Autoridades Garantes: Las autoridades administrativas especializadas en materia de protección de datos personales, integradas por:

a) El órgano desconcentrado de la Secretaría de la Contralora General de la Ciudad de México, con autonomía técnica y de gestión en el ejercicio de sus atribuciones en materia de protección de datos personales;

b) El órgano especializado del Poder Legislativo;

c) El órgano especializado del Poder Judicial; y

d) Los órganos especializados de los organismos constitucionales autónomos de la Ciudad de México.

Para el cumplimiento de sus atribuciones en materia de protección de datos personales, las Autoridades Garantes actuarán con independencia técnica en sus resoluciones, libres de presión, influencia o injerencia indebida de autoridades jerárquicamente superiores, y sus determinaciones se adoptarán conforme exclusivamente a criterios jurídicos y técnicos especializados.

Las Autoridades Garantes contarán con personal profesional especializado en protección de datos personales cuya designación, remoción y ejercicio de funciones se regirá por criterios de mérito, capacidad técnica e imparcialidad.

IV. Aviso de privacidad: Documento a disposición de la persona titular de forma física, electrónica o en cualquier formato generado por el Sujeto obligado, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

V. Bases de datos: Conjunto ordenado de información personal que estén en posesión del Sujeto obligado, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

VI. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, 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, y en su caso supresión, en la base de datos que corresponda;

VII. Catálogo de bases de datos personales: Lista detallada del conjunto ordenado de información personal en posesión del Sujeto obligado, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

VIII. Comité de Transparencia: Órgano colegiado encargado de supervisar, vigilar y coordinar los procedimientos en materia de protección de datos personales;

IX. Cómputo en la nube: Modelo de provisión externa de servicios electrónicos bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

X. Consentimiento: Manifestación de la voluntad libre, específica e informada de la persona titular, de forma tácita o expresa, mediante la cual autoriza el tratamiento de sus datos personales;

XI. Datos personales: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

XII. Datos personales sensibles: Aquella que se refiera a la esfera más íntima de la persona titular, vida afectiva o familiar, o 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 el origen racial o étnico, estado de salud físico o mental ya sea presente o futuro, información genética, creencias religiosas, filosóficas y morales, filiación sindical, opiniones políticas y/o preferencia sexual;

XIII. Derechos ARCO Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, en los términos definidos por la Ley General;

XIV. Derecho de protección de datos: El derecho para decidir sobre el uso y manejo de la información personal, por el que se imponen obligaciones a las instituciones públicas y a los particulares que utilizan datos personales, a fin de garantizar el buen uso de los mismos y el respeto a la privacidad;

XV. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse a la persona titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;



XVI. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de protección técnicas, físicas y administrativas adoptadas por el Sujeto obligado para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XVII. Evaluación de impacto en la protección de datos personales: Documento mediante el cual los Sujetos obligados valoran las repercusiones reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de las personas titulares de los derechos ARCO, así como los deberes de los Sujetos obligados y de las personas encargadas, previstos en la normativa aplicable;

XVIII. Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, 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, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;

XIX. Inventario de datos personales: Lista ordenada y detallada que posea el Sujeto obligado o la persona encargada, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable;

XX. Ley: Ley de Protección de Datos Personales en Posesión de Sujetos obligados del Ciudad de México;

XXI. Ley de Transparencia: Ley de Transparencia y Acceso a la Información Pública para el Ciudad de México;

XXII. Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

XXIII. Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública;

XXIV. Medidas compensatorias: Mecanismos alternos para dar a conocer a las personas titulares de los derechos ARCO, el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

XXV. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XXVI. Medidas de seguridad administrativas: Políticas, acciones 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;

XXVII. Medidas de seguridad físicas: Conjunto de 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 deben considerar las siguientes actividades: 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; y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

XXVIII. Medidas de seguridad técnicas: Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea solamente 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; y

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

XXIX. Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 44 de la Ley General de Transparencia;

XXX. Persona encargada: Persona física o jurídica, pública o privada, ajena a la organización del Sujeto obligado, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del Sujeto obligado;

XXXI. Persona titular: La persona física a quien corresponden los datos personales;

XXXII. Portabilidad La facultad de la persona titular, prevista en la Ley General, de obtener los datos personales que haya facilitado y que se conserven en sistemas de tratamiento automatizado de los Sujetos obligados, en un formato estructurado y de uso común, para su transmisión a otro Sujeto obligado cuando sea técnicamente posible, conforme a los lineamientos que emita el Sistema Nacional de Transparencia;





XXXIII. Remisión: Toda comunicación de datos personales realizada exclusivamente entre el Sujeto obligado y la persona encargada, dentro o fuera del territorio mexicano;

XXXIV. Sistema de gestión: 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 que le resulten aplicables en la materia;

XXXV. Sistema Local: Sistema de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México;

XXXVI. Sujetos obligados: Cualquier autoridad, agencia, comisión, comité, corporación, ente, entidad, institución, órgano, organismo o equivalente de los poderes Ejecutivo, Legislativo y Judicial de la Ciudad de México, las Alcaldías, organismos públicos autónomos y fideicomisos públicos;

XXXVII. Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la persona titular, del Sujeto obligado o de la persona encargada;

XXXVIII. Transmisión: Para efectos de esta Ley, se entenderá por transmisión la comunicación de datos personales realizada entre el Sujeto obligado y un tercero receptor que actúe como nuevo responsable del tratamiento, distinta de la remisión efectuada exclusivamente entre el Sujeto obligado y la persona encargada. En todo lo no regulado por esta definición, se aplicarán supletoriamente los artículos de la Ley General relativos a transferencia de datos personales;

XXXIX. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, publicación, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales; y

XL. Unidad de Transparencia: La instancia que funge como el vínculo entre el Sujeto obligado y la persona titular, la cual tendrá a su cargo la recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO.

**Artículo 4.** La presente Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos de los Sujetos obligados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.



Para garantizar la tutela efectiva del derecho a la protección de datos personales, las Autoridades Garantes observarán las siguientes garantías institucionales:

**I. Independencia técnica:** Las resoluciones en materia de protección de datos personales se adoptarán conforme exclusivamente a criterios jurídicos, técnicos y de derechos humanos, libres de presión, influencia o injerencia indebida de autoridades jerárquicamente superiores;

**II. Especialización:** El personal que ejerza funciones de resolución en materia de protección de datos personales deberá acreditar formación especializada en la materia y experiencia profesional comprobable;

**III. Estabilidad:** El personal especializado no podrá ser removido de sus funciones sino por causas graves debidamente fundadas y motivadas, conforme a procedimientos que garanticen audiencia y debido proceso;

**IV. Transparencia:** Las Autoridades Garantes publicarán sus resoluciones en versión pública, criterios de interpretación, estadísticas de cumplimiento y evaluaciones de impacto institucional;

**V. Prohibición de conflicto de interés:** Las personas que integren o colaboren con las Autoridades Garantes se excusarán de conocer asuntos en los que exista conflicto de interés, vinculación directa con el Sujeto obligado o impedimento legal;

**VI. Deber de fundamentación reforzada:** Las resoluciones que nieguen, limiten o restrinjan derechos de las personas titulares deberán estar exhaustivamente fundadas y motivadas, con aplicación del principio pro persona y ponderación explícita de derechos en conflicto;

**VII. Coordinación institucional:** Las Autoridades Garantes establecerán mecanismos de coordinación, homologación de criterios y construcción de jurisprudencia administrativa uniforme en materia de protección de datos personales, bajo la coordinación del Sistema Nacional de Transparencia.

Las autoridades de las que dependan administrativamente las Autoridades Garantes se abstendrán de interferir, obstaculizar o condicionar el ejercicio de las atribuciones especializadas en materia de protección de datos personales.

Cualquier acto que vulnere la independencia técnica de las Autoridades Garantes en el ejercicio de sus atribuciones especializadas será nulo de pleno derecho y constituirá causa de responsabilidad administrativa.

**Artículo 5.** Para los efectos de la presente Ley, se considerarán como fuentes de acceso público:



I. Las páginas de internet, medios remotos o 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, periódicos, gacetas o boletines oficiales, de acuerdo con su normativa;

IV. Los medios de comunicación social; y

V. Los registros públicos conforme a las disposiciones que les resulten aplicables. Para que los supuestos enumerados en el presente artículo sean considerados fuentes de acceso público será necesaria que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contra prestación, derecho o tarifa.

No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.

**Artículo 6.** El Estado o el Sujeto obligado garantizará el derecho a la privacidad de las y los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

El derecho a la protección de datos personales solamente se limitará por disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceras personas.

**Artículo 7.** Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de la persona titular o en su defecto, se trate de los casos establecidos en el artículo 62 de esta Ley.

En el tratamiento de datos personales de niñas, niños o adolescentes, se deberá privilegiar su interés superior, en los términos de esta Ley y demás disposiciones legales aplicables.

**Artículo 8.** La aplicación e interpretación de la presente Ley se realizará conforme a las bases y principios establecidos en la Constitución Política de los Estados Unidos Mexicanos, los instrumentos jurídicos internacionales ratificados por nuestro país, la Constitución Política del Ciudad de México y la Ley General.

**Artículo 9.** La Ley de Procedimiento Administrativo del Ciudad de México se aplicarán de manera supletoria en todo lo no previsto por esta Ley.



## TÍTULO SEGUNDO DE LOS DERECHOS DE LAS PERSONAS TITULARES Y SU EJERCICIO

### CAPÍTULO ÚNICO DE LOS DERECHOS DE PROTECCIÓN DE DATOS PERSONALES

**Artículo 10.** En todo momento la persona titular o su representante podrán solicitar al Sujeto obligado, el ejercicio de los derechos ARCO al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente capítulo.

El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impedimento para el ejercicio de otro de ellos.

**Artículo 11.** La persona titular tendrá derecho de acceder a sus datos personales que obren en posesión del Sujeto obligado, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

**Artículo 12.** La persona titular tendrá derecho a solicitar al Sujeto obligado la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

**Artículo 13.** La persona titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del Sujeto obligado, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

**Artículo 14.** La persona titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese el mismo, cuando:

I. Aún siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio a la persona titular, y

II. 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.

**Artículo 15.** La persona titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una





solicitud de rectificación u oposición hasta su resolución por el Sujeto obligado o se encuentre en sustanciación un recurso de revisión.

La persona titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento, aún cuando éstos sean innecesarios para el Sujeto obligado, en caso de que la persona titular los requiera para formular una inconformidad o procedimiento análogo.

## **TÍTULO TERCERO DE LAS AUTORIDADES RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS**

### **CAPÍTULO PRIMERO DE LOS SUJETOS OBLIGADOS**

**Artículo 16.** Son Sujetos obligados por esta Ley:

- I. El Poder Ejecutivo de la Ciudad de México, sus dependencias y entidades;
- II. El Poder Judicial de la Ciudad de México y los órganos que lo integran;
- III. El Poder Legislativo de la Ciudad de México y los órganos que lo integran;
- IV. Las Alcaldías de la Ciudad de México, sus dependencias y entidades; y
- V. Los organismos públicos autónomos de la Ciudad de México.

En términos de esta Ley, quedan exceptuados los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito de la Ciudad de México y de las Alcaldías, los cuales serán responsables de la protección de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de particulares.

**Artículo 17.** El Sujeto obligado deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

### **SECCIÓN I DE LAS OBLIGACIONES**

**Artículo 18.** El Sujeto obligado deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por la persona 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, deberán ser suprimidos, previo bloqueo en su caso, una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

**Artículo 19.** El Sujeto obligado deberá establecer y documentar los procedimientos o acciones para la conservación y, en su caso, 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 de la presente Ley.

En los procedimientos a que se refiere el párrafo anterior, el Sujeto obligado deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.

**Artículo 20.** El Sujeto obligado sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

**Artículo 21.** El Sujeto obligado deberá informar a la persona titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el Sujeto obligado.

Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla.

Cuando resulte imposible dar a conocer a la persona titular el aviso de privacidad de manera directa, o ello exija esfuerzos desproporcionados, el Sujeto obligado podrá instrumentar medidas compensatorias de comunicación masiva.

**Artículo 22.** El Sujeto obligado deberá implementar los mecanismos previstos en el artículo siguiente para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley, y rendir cuentas sobre el



tratamiento de datos personales en su posesión, a la persona titular o a las Autoridades Garantes, según corresponda.

**Artículo 23.** Entre los mecanismos que deberá adoptar el Sujeto obligado para cumplir con el principio de responsabilidad están, al menos, los siguientes:

I. Destinar recursos autorizados, 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 Sujeto obligado;

III. Poner en práctica programas 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 externa, 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 las personas 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 que resulten aplicables en la materia; y

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 defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

**Artículo 24.** A efecto de facilitar el ejercicio de los derechos previstos en el Título Cuarto, Capítulo Primero, los Sujetos obligados deberán notificar a la Autoridad Garante, según su competencia, los inventarios de datos personales y los catálogos de base de datos personales que posean, la categoría de datos de que se componen, su finalidad, la normatividad que les resulte aplicable; así como la persona encargada y las áreas en la que se encuentran dichos datos.

**Artículo 25.** Para el cumplimiento de las obligaciones previstas en la presente Ley, el Sujeto obligado podrá desarrollar o adoptar, en lo individual o en



de acuerdo con otros Sujetos obligados, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto:

- I. Elevar el nivel de protección de los datos personales, en especial los datos personales de los menores de edad;
- II. Identificar cuando se traten datos personales sensibles;
- III. Armonizar el tratamiento de datos personales en un sector específico;
- IV. Facilitar a las personas titulares el ejercicio de los derechos ARCO;
- V. Facilitar las transmisiones y transferencias de datos personales;
- VI. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales; y
- VII. Demostrar ante las Autoridades Garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

**Artículo 26.** Todo esquema de mejores prácticas que busque la validación o reconocimiento por parte de las Autoridades Garantes deberá:

- I. Cumplir con los criterios y parámetros que para tal efecto emita la Autoridad Garante que corresponda según su ámbito de competencia; y
- II. Ser notificado ante las Autoridades Garantes de conformidad con el procedimiento establecido en los parámetros señalados en la fracción anterior, a fin de que sean evaluados y, en su caso, validados o reconocidos e inscritos en el registro al que refiere el último párrafo de este artículo.

Las Autoridades Garantes, según su ámbito de competencia, deberán emitir las reglas de operación de los registros en los que se inscribirán aquellos esquemas de mejores prácticas validados o reconocidos.

Las Autoridades Garantes podrán inscribir los esquemas de mejores prácticas que hayan reconocido o validado en el registro administrado por las Autoridades Garantes, de acuerdo con las reglas que fije esta última.

**Artículo 27.** Cuando el Sujeto obligado 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 las Autoridades Garantes, según su ámbito de competencia, el cual podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

El contenido de la evaluación de impacto en la protección de datos personales deberá determinarse por las Autoridades Garantes, en el ámbito de su competencia.





**Artículo 28.** Los Sujetos obligados que realicen una evaluación de impacto en la protección de datos personales, deberá presentarla ante las Autoridades Garantes, según su ámbito de competencia, 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 de que estas, en su caso, emita las recomendaciones no vinculantes correspondientes, en un plazo de treinta días posteriores contados a partir del día siguiente a la presentación de la evaluación.

**Artículo 29.** 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.

**Artículo 30.** Los Sujetos obligados deberán colaborar con las Autoridades Garantes, según corresponda, para capacitar y actualizar de forma permanente a todas las personas servidoras públicas 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.

## **SECCIÓN II DE LA RELACIÓN DEL SUJETO OBLIGADO Y DE LA PERSONA ENCARGADA**

**Artículo 31.** La persona encargada deberá realizar 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 Sujeto obligado de conformidad con los principios y bases que establece la presente Ley.

**Artículo 32.** La relación entre el Sujeto obligado y la persona encargada deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el Sujeto obligado, 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 Sujeto obligado se deberán prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste la persona encargada:





- I. Realizar el tratamiento de los datos personales conforme a las instrucciones del Sujeto obligado;
- II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Sujeto obligado;
- III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- IV. Informar al Sujeto obligado cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
- V. Guardar confidencialidad respecto de los datos personales tratados;
- VI. Devolver y/o suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el Sujeto obligado, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales; y
- VII. Abstenerse de transferir o transmitir los datos personales salvo en el caso de que el Sujeto obligado así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

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

**Artículo 33.** Cuando la persona encargada incumpla las instrucciones del Sujeto obligado y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de Sujeto obligado conforme a la legislación en la materia que le resulte aplicable.

**Artículo 34.** La persona encargada podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del Sujeto obligado, siempre y cuando medie la autorización expresa de este último.

La persona subcontratada asumirá el carácter de persona encargada en los términos de la presente Ley y demás disposiciones que resulten aplicables en la materia.

Cuando el contrato o el instrumento jurídico mediante el cual se haya formalizado la relación entre el Sujeto obligado y la persona encargada prevea que éste 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.

**Artículo 35.** Una vez obtenida la autorización expresa del Sujeto obligado, la persona encargada deberá formalizar la relación adquirida con la persona





subcontratada 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.

**Artículo 36.** El Sujeto obligado 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 la persona proveedora externa garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

En su caso, el Sujeto obligado deberá delimitar el tratamiento de los datos personales por parte de la persona proveedora externa a través de cláusulas contractuales u otros instrumentos jurídicos.

**Artículo 37.** Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el Sujeto obligado se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que la persona proveedora:

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 preste el servicio; y

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

II. Cuenten con mecanismos, al menos, para:

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

b) Permitir al Sujeto obligado 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 Sujeto obligado y que este último haya podido recuperarlos; e

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

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

## CAPÍTULO SEGUNDO DEL COMITÉ DE TRANSPARENCIA

**Artículo 38.** Cada Sujeto obligado contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia y demás normativa aplicable.

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

**Artículo 39.** Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en las áreas del Sujeto obligado, 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 de 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 las Autoridades Garantes, según corresponda;





VII. Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales; y

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

### CAPÍTULO TERCERO DE LA UNIDAD DE TRANSPARENCIA

**Artículo 40.** Cada Sujeto obligado contará con una Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley de Transparencia, esta Ley y demás normatividad aplicable y tendrá en materia de datos personales, las siguientes funciones:

I. Auxiliar y orientar a la persona 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 solo se entreguen a la persona titular o su representante debida y legalmente acreditado;

IV. Informar a la persona 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 una 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; y

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

Los Sujetos obligados que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a una persona oficial de protección de datos personales, especializada en la materia, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia. Los Sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de las respuestas a solicitudes de información en materia de datos personales, en cualquier formato accesible que corresponda, de conformidad con la Ley General.





**Artículo 41.** El Sujeto obligado procurará que las personas o grupos de atención prioritaria, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales, de conformidad con la Ley General.

## **CAPÍTULO CUARTO DE LAS AUTORIDADES GARANTES**

**Artículo 42.** Además de las atribuciones que les confiere el artículo 83 de la Ley General, corresponderá a las Autoridades Garantes las siguientes:

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

II. Impulsar en conjunto con instituciones de educación 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 las Autoridades Garantes en sus tareas sustantivas;

III. 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 Sujetos obligados;

IV. Aplicar, en el ámbito de la Ciudad de México, los criterios que determine el Sistema Nacional de Transparencia para identificar tratamientos intensivos o relevantes de datos personales. Cuando el Sistema Nacional no haya emitido criterios específicos sobre una materia, las Autoridades Garantes podrán emitir criterios complementarios de carácter provisional, los cuales deberán notificarse al Sistema Nacional de Transparencia para su conocimiento y, en su caso, homologación; y

V. Las demás que le confiera la presente Ley y demás disposiciones aplicables.

## **TÍTULO CUARTO DE LOS PROCEDIMIENTOS ADMINISTRATIVOS EN MATERIA DE DATOS PERSONALES**

### **CAPÍTULO PRIMERO DE LOS PROCEDIMIENTOS PARA EL EJERCICIO DE LOS DERECHOS ARCO**

**Artículo 43.** Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del Sujeto obligado competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezcan las Autoridades Garantes, en el ámbito de sus respectivas competencias.





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

**Artículo 44.** Las Autoridades Garantes, según corresponda, podrán establecer formularios, sistemas y otros métodos simplificados para facilitar a las personas titulares el ejercicio de los derechos ARCO. Los medios y procedimientos habilitados por el Sujeto obligado 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 las personas titulares y la forma en que mantienen contacto cotidiano o común con el Sujeto obligado.

**Artículo 45.** Cuando el Sujeto obligado no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento de la persona titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el Sujeto obligado competente.

**Artículo 46.** En caso de que la persona encargada declare inexistencia de los datos personales en sus archivos, registros, sistemas o expedientes, dicha declaración deberá constar en una resolución del Comité de Transparencia del Sujeto obligado en términos de la Ley de Transparencia.

En caso de que el Sujeto obligado advierta que la solicitud para el ejercicio de los derechos ARCO corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento a la persona titular.

**Artículo 47.** La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a los Sujetos obligados, se sujetarán al procedimiento establecido en el presente capítulo y demás disposiciones que resulten aplicables en la materia.

**Artículo 48.** Para el ejercicio de los derechos ARCO será necesario acreditar la identidad de la persona titular, y en su caso, la identidad y personalidad con la que actúe el representante.

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, y 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.

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente Capítulo, siempre y cuando no exista mandato judicial o disposición legal en contrario.

**Artículo 49.** El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable.

Para efectos de acceso a datos personales, las leyes que establezcan los costos de reproducción y certificación deberán considerar en su determinación que los montos permitan o faciliten el ejercicio de este derecho.

Cuando la persona titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a éste. La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte copias simples. Las Unidades de Transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas de la persona titular.

El Sujeto obligado no podrá establecer, para la presentación de las solicitudes del ejercicio de los derechos ARCO, algún servicio o medio que implique un costo a la persona titular.

**Artículo 50.** El Sujeto obligado deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo 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 a la persona titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio de los derechos ARCO, el Sujeto obligado 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 a la persona titular.

**Artículo 51.** En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:

I. El nombre de la persona titular y su domicilio o cualquier otro medio para recibir notificaciones;



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

III. De ser posible, el área encargada 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 la persona titular; y

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

Cuando se trate de una solicitud de acceso a datos personales, la persona titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan.

El Sujeto obligado deberá atender la solicitud en la modalidad requerida por la persona 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.

**Artículo 52.** En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el artículo anterior y las Autoridades Garantes no cuenten con elementos para subsanarla, se prevendrá a la persona titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los 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 los derechos ARCO. La prevención tendrá el efecto de interrumpir el plazo que tiene el Sujeto obligado, para resolver la solicitud de ejercicio de los derechos ARCO.

**Artículo 53.** Con relación a una solicitud de cancelación, la persona titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del Sujeto obligado.

El Sujeto obligado podrá cancelar sin suprimir los datos personales, siempre y cuando sean considerados los aspectos administrativos, contables, fiscales, jurídicos e históricos y funde y motive la imposibilidad.



**Artículo 54.** En el caso de la solicitud de oposición, la persona titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

**Artículo 55.** Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un procedimiento específico para solicitar el ejercicio de los derechos ARCO, el Sujeto obligado deberá informar la persona titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce sus derechos a través del procedimiento específico institucionalizado, o bien, por medio del procedimiento para la atención de solicitudes para el ejercicio de los derechos ARCO conforme a las disposiciones establecidas en este Capítulo.

**Artículo 56.** Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:

I. Cuando la persona titular o su representante no estén debidamente acreditados para ello;

II. Cuando los datos personales no se encuentren en posesión del Sujeto obligado;

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 Sujeto obligado no sea competente;

IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados de la persona titular;

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

En todos los casos anteriores, el Sujeto obligado deberá informar a la persona titular el motivo de su determinación, en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 50 de la presente Ley y demás disposiciones aplicables, y por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.





## CAPÍTULO SEGUNDO DEL TRATAMIENTO DE LOS DATOS PERSONALES

**Artículo 57.** El tratamiento de datos personales por parte del Sujeto obligado deberá sujetarse a las facultades y/o atribuciones que la normatividad aplicable le confiera.

**Artículo 58.** Todo tratamiento de datos personales que efectúe el Sujeto obligado deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

El Sujeto obligado podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la Ley y medie el consentimiento de la persona titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

**Artículo 59.** El Sujeto obligado no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses de la persona titular y la expectativa razonable de privacidad.

**Artículo 60.** Cuando no se actualice alguna de las causales de excepción previstas en el artículo 62 de la presente Ley, el Sujeto obligado deberá contar con el consentimiento previo de la persona titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

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

II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e

III. Informada: Que la persona titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos.

En la obtención del consentimiento de niñas, niños o adolescentes; o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la Ley, se deberá recabar el consentimiento por escrito, de quienes ejerzan la patria potestad o tutela, así como la opinión de la niña, niño o adolescente, respectivamente.

La persona encargada realizará esfuerzos razonables para verificar que el consentimiento fue otorgado por la persona titular de la patria potestad o tutela, teniendo en cuenta los medios y la tecnología disponible.



En el caso de que no sea posible recabar el consentimiento de quienes ejerzan la patria potestad o tutela de una o un adolescente, éste podrá otorgarlo siempre que ello no implique una afectación a sus derechos.

Cualquier comunicación pública sobre la identificación de restos humanos deberá realizarse por razones estrictas de interés público, previo consentimiento expreso y por escrito de las familias afectadas y en respeto pleno a sus derechos.

**Artículo 61.** El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad de la persona titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

El consentimiento será tácito cuando habiéndose puesto a disposición de la persona 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 aplicables exijan que la voluntad de la persona titular se manifieste expresamente. Tratándose de datos personales sensibles y datos personales niñas, niños o adolescentes, el Sujeto obligado deberá obtener el consentimiento expreso y por escrito de la persona titular o de quien ejerza la patria potestad o tutela en su caso, 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 el artículo 62 de esta Ley.

**Artículo 62.** El Sujeto obligado no estará obligado a recabar el consentimiento de la persona titular para el tratamiento de sus datos personales, exclusivamente en los siguientes casos, los cuales deberán interpretarse de manera estricta y no analógica:

I. Cuando una ley así lo disponga expresamente, siempre que los supuestos sean acordes con las bases y principios de la Ley General y la presente Ley;

II. Cuando las transferencias entre Sujetos obligados recaigan sobre datos personales necesarios para el ejercicio de facultades expresamente conferidas por disposición legal al Sujeto obligado receptor, respecto de las mismas finalidades que motivaron el tratamiento original;

III. Cuando exista orden judicial o resolución fundada y motivada de autoridad competente;

IV. Para el reconocimiento o defensa de derechos de la persona titular ante autoridad competente;

V. Cuando los datos personales sean estrictamente necesarios para el cumplimiento de obligaciones que la normatividad aplicable impone expresamente





al Sujeto obligado en el marco de una relación jurídica con la persona titular, sin que ello comprenda el tratamiento para finalidades distintas a las que originaron dicha relación;

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, o la prestación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación; o

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

## SECCIÓN I DEL TRATAMIENTO DE DATOS PERSONALES PARA LA BÚSQUEDA Y LOCALIZACIÓN DE PERSONAS DESAPARECIDAS, E IDENTIFICACIÓN DE PERSONAS FALLECIDAS

**Artículo 63.** Además de todo lo contenido en la presente Ley, las autoridades competentes, responsables y encargados que den tratamiento a datos personales y datos personales sensibles de personas desaparecidas, familiares, y personas interesadas en la búsqueda efectiva y localización de personas desaparecidas e identificación de personas fallecidas, deberán de observar lo requerido en la presente Sección.

**Artículo 64.** Cualquier persona interesada, podrá otorgar información correspondiente a datos personales de una tercera persona a las autoridades competentes, cuando ésta, se presuma como persona desaparecida, con el fin de que dicha información sea utilizada únicamente para el procedimiento de búsqueda y localización de personas desaparecidas e identificación de personas fallecidas.

El Sujeto obligado y/o la persona encargada deberán realizar esfuerzos razonables para verificar que la información proporcionada por las personas familiares e interesadas, sea veraz y oportuna.

**Artículo 65.** Las autoridades competentes deberán contar con un protocolo de actuación específico para el tratamiento de datos personales y datos personales sensibles, correspondientes a personas desaparecidas, personas familiares, e interesadas, el cual deberá contener por lo menos lo siguiente:

I. El Aviso de privacidad referido en el artículo 71 de la presente Ley, en el cual se encuentre identificada la finalidad única para la cual se está recabando la información.





- II. El proceso que se llevará a cabo para recabar la información.
- III. La obligación expresa de la autoridad competente de explicar de forma clara y accesible el contenido del aviso de privacidad.

**Artículo 66.** Toda la información que contenga datos personales y datos personales sensibles de personas desaparecidas, familiares e interesadas de las mismas, así como de personas fallecidas sin identificar y que sea recabada y tratada por el Sujeto obligado y/o la persona encargada, deberá concentrarse dentro del Sistema de Gestión de Información de Personas Desaparecidas y Personas Fallecidas, regulado por la Ley para la Localización, Recuperación e Identificación Forense de Personas del Ciudad de México.

Las autoridades deberán garantizar que toda información que sea proporcionada voluntariamente con la finalidad de búsqueda y localización de personas desaparecidas e identificación de personas fallecidas, sea utilizada únicamente para este fin.

**Artículo 67.** El Sujeto obligado y/o la persona encargada deberá de establecer y aplicar las medidas de seguridad necesarias previstas en esta Ley, para asegurar que los datos personales y datos personales sensibles contenidos en el Sistema de Gestión de Información de Personas Desaparecidas y Personas Fallecidas, sean utilizados únicamente con la finalidad de la búsqueda efectiva y localización de personas desaparecidas, e identificación de personas fallecidas.

**Artículo 68.** Queda prohibida la transmisión o transferencia de los datos personales y datos personales sensibles contenidos en el Sistema de Gestión de Información de Personas Desaparecidas y Personas Fallecidas, para fines distintos a los mencionados en el artículo anterior.

**Artículo 69.** Cuando la transferencia y/o transmisión de datos personales y datos personales sensibles contenidos en el Sistema de Gestión de Información de Personas Desaparecidas y Personas Fallecidas, sea necesaria para el cumplimiento de la finalidad establecida, el Sujeto obligado y/o la persona encargada deberá aplicar mecanismos que garanticen la confidencialidad de los datos personales.

**Artículo 70.** Las autoridades competentes, podrán cotejar la información contenida en el Sistema de Gestión de Información de Personas Desaparecidas y Personas Fallecidas, con otras bases de datos, según lo reconocido en el artículo 36 de la Ley para la Localización, Recuperación e Identificación Forense de





Personas de la Ciudad de México, con el único fin de la búsqueda efectiva y localización de personas desaparecidas e identificación de personas fallecidas.

Las autoridades competentes deberán informar a la persona familiar o interesada toda la información necesaria, cuando se realice el cotejo de los datos personales y datos personales sensibles conforme al párrafo anterior.

**Artículo 71.** El Sujeto obligado y/o la persona encargada, deberá emitir un Aviso de Privacidad específico para el tratamiento de la información que será recabada conforme al protocolo de actuación mencionado en el artículo 65 del presente ordenamiento, para la búsqueda y localización de personas desaparecidas e identificación de personas fallecidas, el cual deberá de contener, además de lo establecido en los artículos 90 y 91 de la presente Ley, lo siguiente:

I. El domicilio de la persona encargada y del Sujeto obligado de los datos personales y datos personales sensibles;

II. Como finalidad del tratamiento para la cual se obtienen los datos personales y datos personales sensibles, se establecerá específica y únicamente, la búsqueda y localización de personas desaparecidas e identificación de personas fallecidas;

III. Los mecanismos, medios y procedimientos que tendrán disponibles los familiares e interesados para ejercer los derechos ARCO;

IV. Los medios a través de los cuales el Sujeto obligado y/o la persona encargada comunicará a los familiares e interesados, la información adicional relativa al aviso privacidad; y

V. Los medios a través de los cuales el Sujeto obligado y/o la persona encargada comunicará a los familiares e interesados, cualquier información en relación con la búsqueda efectiva y localización de las personas desaparecidas e identificación de las personas fallecidas.

**Artículo 72.** Una vez puesto a disposición el aviso de privacidad mencionado en el artículo anterior, y explicado de manera clara y accesible el contenido del mismo, el Sujeto obligado o la persona encargada deberá recabar el consentimiento informado, expreso y por escrito del familiar o interesado conforme al proceso señalado dentro del protocolo de actuación referido en el artículo 65 de la presente Ley.

El Sujeto obligado y/o la persona encargada no estará obligado a recabar el consentimiento de la persona familiar o interesada para el tratamiento de datos personales, cuando se actualicen alguna de las excepciones del artículo 62 de la presente Ley.



**Artículo 73.** Tratándose de datos personales y datos personales sensibles cuya persona titular sea una persona desaparecida o fallecida se tendrá a lo dispuesto por el artículo 48 de la presente Ley para el ejercicio de los derechos ARCO contenidos en la misma.

**Artículo 74.** Cualquier comunicación pública sobre la localización de personas desaparecidas o la identificación de restos humanos deberá realizarse por razones estrictas de interés público, previo consentimiento expreso y por escrito de las familias afectadas y en respeto pleno a sus derechos.

**Artículo 75.** El honor y el respeto a la imagen de personas desaparecidas y personas fallecidas, se protegerán en beneficio de sus familiares y personas interesadas, así como se deberá proteger el honor y el respeto de éstos últimos.

**Artículo 76.** Toda la información relativa a datos personales y datos personales sensibles a que refiere esa Sección, es considerada información confidencial y especialmente protegida conforme a la legislación en la materia.

## **SECCIÓN II DE LAS BASES DE DATOS EN POSESIÓN DE INSTANCIAS DE SEGURIDAD, PROCURACIÓN Y ADMINISTRACIÓN DE JUSTICIA**

**Artículo 77.** La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de los Sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, 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 las bases de datos que ellos mismos establezcan para tal efecto.

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

**Artículo 78.** En el tratamiento de datos personales, así como en el uso de las bases de datos para su almacenamiento, que realicen los Sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia, se deberá 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 correspondiente





o de la persona titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.

**Artículo 79.** Los Sujetos obligados de las bases de datos a que se refiere esta Sección, deberán establecer medidas de seguridad de alto nivel, 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.

### SECCIÓN III DE LAS MEJORES PRÁCTICAS

**Artículo 80.** 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; y
- III. Se efectúen o pretendan efectuar transmisiones o transferencias de datos personales.

**Artículo 81.** La Autoridad Garante, en el ámbito de su competencia, podrá emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales, en función de:

- I. El número de personas titulares;
- II. El público objetivo; y
- III. El desarrollo de la tecnología utilizada.

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

## CAPÍTULO TERCERO DE LAS TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES

**Artículo 82.** La persona titular podrá ejercer el derecho de portabilidad respecto de los datos personales que haya facilitado y que obre en sistemas de tratamiento automatizado de los Sujetos obligados, de conformidad con lo establecido en la Ley General y los lineamientos técnicos que para tal efecto emita el Sistema Nacional de Transparencia.

Los Sujetos obligados adecuarán sus sistemas y procesos para dar cumplimiento al ejercicio de este derecho en los plazos y modalidades que determinen los lineamientos referidos en el párrafo anterior. En ningún caso el plazo de respuesta será superior al previsto en el artículo 50 de esta Ley.





**Artículo 83.** Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de la persona titular, salvo las excepciones previstas en los artículos 62, 84 y 88, de esta Ley.

**Artículo 84.** Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al Sujeto obligado, 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 siguientes casos:

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

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 receptor, siempre y cuando las facultades entre el Sujeto obligado transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del Sujeto obligado transferente.

**Artículo 85.** Cuando la transferencia sea nacional, el receptor de los datos personales los deberá tratar comprometiéndose 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 Sujeto obligado transferente conforme lo establecido por la Ley General.

**Artículo 86.** El Sujeto obligado sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o la persona encargada se obligue a proteger los datos personales conforme a los principios y deberes que establece la Ley General, la presente Ley y las disposiciones que resulten aplicables en la materia.

**Artículo 87.** En toda transferencia de datos personales, el Sujeto obligado deberá comunicar al receptor, el aviso de privacidad conforme al cual se tratan dichos datos frente a la persona titular.



**Artículo 88.** El Sujeto obligado podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento de la persona titular, en los siguientes supuestos:

I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;

II. Cuando la transferencia se realice entre Sujetos obligados, 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 Sujeto obligado y la persona titular;

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés de la persona titular, por el Sujeto obligado y un tercero; y

VIII. Cuando se trate de los casos en los que el Sujeto obligado no esté obligado a recabar el consentimiento de la persona titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 62 de la presente Ley.

La actualización de algunas de las excepciones previstas en este artículo, no exime al Sujeto obligado de cumplir con las obligaciones previstas en el presente Capítulo que resulten aplicables.

**Artículo 89.** Las remisiones nacionales e internacionales de datos personales que se realicen entre Sujeto obligado y la persona encargada no requerirán ser informadas a la persona titular, ni contar con su consentimiento.

## CAPÍTULO CUARTO AVISO DE PRIVACIDAD

**Artículo 90.** El aviso de privacidad se pondrá a disposición de la persona titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información:





- I. La denominación del Sujeto obligado;
- II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento de la persona titular;
- III. Cuando se realicen transmisiones o transferencias de datos personales que requieran consentimiento, se deberá informar: a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren o transmiten los datos personales; y b) Las finalidades de estas transferencias o transmisiones;
- IV. Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades o transferencias y transmisiones de datos personales que requieren el consentimiento de la persona titular; y
- V. El sitio donde se podrá consultar el aviso de privacidad integral.

El poner a disposición el aviso de privacidad al que refiere este artículo, no exime al Sujeto obligado de su obligación de proveer los mecanismos para que la persona titular pueda conocer el contenido del aviso de privacidad al que se refiere el artículo siguiente.

Los mecanismos y medios a los que se refiere la fracción IV de este artículo, deberán estar disponibles para que la persona titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias y transmisiones que requieran el consentimiento de la persona titular, previo a que ocurra dicho tratamiento.

**Artículo 91.** El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo anterior, deberá contener, al menos, la siguiente información:

- I. El domicilio del Sujeto obligado;
- II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
- III. El fundamento legal que faculta al Sujeto obligado para llevar a cabo el tratamiento;
- IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento de la persona titular;
- V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO de los datos personales;
- VI. El domicilio de la Unidad de Transparencia del Sujeto obligado; y
- VII. Los medios a través de los cuales el Sujeto obligado comunicará a las personas titulares los cambios al aviso de privacidad.



## CAPÍTULO QUINTO DE LAS MEDIDAS DE SEGURIDAD

**Artículo 92.** Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el Sujeto obligado deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

**Artículo 93.** Las medidas de seguridad adoptadas por el Sujeto obligado deberán considerar:

- 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 personas titulares;
- V. Las transferencias y transmisiones de datos personales que se realicen;
- VI. El número de las personas titulares;
- VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento; y
- 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.

**Artículo 94.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto obligado deberá realizar, al menos, las siguientes actividades interrelacionadas:

- 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 los 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 Sujeto obligado, entre otros.





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

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 vulneraciones a las que están sujetos los datos personales; y

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.

**Artículo 95.** Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

**Artículo 96.** De manera particular, el Sujeto obligado deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

- I. El inventario de datos personales y de los sistemas de tratamiento;
- II. Las funciones y obligaciones de las personas que traten datos personales;
- III. El análisis de riesgos;
- IV. El análisis de brecha;
- V. El plan de trabajo;
- VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad; y
- VII. Los programas de capacitación y actualización.

**Artículo 97.** El Sujeto obligado deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

- 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; e
- IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

**Artículo 98.** En caso de que se vulnere la seguridad de los datos personales, el Sujeto obligado deberá analizar 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 vulneración se repita.

**Artículo 99.** Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos personales, al menos, las siguientes:

- I. La pérdida, el robo, extravío, o daño de datos personales;
- II. La copia, o destrucción no autorizada;
- III. El uso, acceso o tratamiento no autorizado; o
- IV. La alteración o modificación no autorizada.

**Artículo 100.** El Sujeto obligado deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

**Artículo 101.** El Sujeto obligado deberá informar sin dilación alguna a la persona titular, y a las Autoridades Garantes, según correspondan, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el Sujeto obligado haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que las personas titulares afectadas puedan tomar las medidas correspondientes para la defensa de sus derechos.

**Artículo 102.** El Sujeto obligado deberá informar a la persona titular al menos lo siguiente:

- I. La naturaleza del incidente;
- II. Los datos personales comprometidos;
- III. Las recomendaciones a la persona titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- IV. Las acciones correctivas realizadas de forma inmediata; y
- V. Los medios donde puede obtener más información al respecto.

**Artículo 103.** El Sujeto obligado deberá establecer controles o mecanismos que tengan por objeto que todas aquellas 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 mismo. Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.





## TÍTULO QUINTO DE LOS MEDIOS DE IMPUGNACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

### CAPÍTULO PRIMERO DEL PROCEDIMIENTO DE VERIFICACIÓN

**Artículo 104.** Las Autoridades Garantes, en el ámbito de su competencia, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ella.

El personal de las Autoridades Garantes estará obligado a guardar estricta confidencialidad sobre la información a la que tenga acceso en virtud de la verificación correspondiente, bajo pena de responsabilidad administrativa, civil y penal.

Los Sujetos obligados facilitarán el acceso a la documentación, sistemas y bases de datos personales requeridos con motivo de una verificación. Cuando la información solicitada esté clasificada como reservada o confidencial conforme a la legislación de transparencia, se aplicarán las siguientes reglas:

a) La Autoridad Garante podrá acceder a dicha información mediante procedimientos que garanticen su protección, incluyendo visualización controlada, análisis in situ sin extracción de copias, o cualquier otro mecanismo que preserve la clasificación;

b) La información clasificada a la que accedan las Autoridades Garantes conservará su carácter de reservada o confidencial y no podrá ser divulgada, publicada ni incorporada al expediente de verificación, salvo en versión pública que elimine los elementos clasificados;

c) Tratándose de información relacionada con violaciones graves a derechos humanos, delitos de lesa humanidad, desaparición forzada o derecho a la verdad, no podrá invocarse clasificación alguna que impida el ejercicio de las facultades de verificación.

El incumplimiento injustificado de los requerimientos de verificación constituirá presunción de veracidad de los hechos denunciados, sin perjuicio de las responsabilidades y sanciones aplicables.

**Artículo 105.** Las verificaciones a que se refiere el presente Capítulo podrán realizarse de oficio o por denuncia cuando se presuma que existen violaciones a las disposiciones a la Ley, o por el sometimiento voluntario de los Sujetos obligados.



**Artículo 106.** Los Sujetos obligados podrán voluntariamente someterse a la realización de revisión por parte de las Autoridades Garantes, 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 normatividad que resulte aplicable.

**Artículo 107.** En las verificaciones solicitadas por los Sujetos obligados a las que se refiere el artículo anterior, la Autoridad Garante rendirá un informe en el que dictaminará sobre la adecuación de las medidas y controles implementados por el Sujeto obligado e identificará sus deficiencias, así como también propondrá acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.

**Artículo 108.** La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte de las Autoridades Garantes, la cual tiene por objeto requerir al Sujeto obligado la documentación e información necesaria vinculada con la presunta violación y/o realizar las visitas a las oficinas o instalaciones del Sujeto obligado, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.

El procedimiento de verificación deberá tener una duración máxima de cincuenta días.

**Artículo 109.** La verificación cuando se presuma que existen violaciones a las disposiciones a la Ley podrá iniciarse:

I. De oficio cuando las Autoridades Garantes cuente con indicios que hagan presumir de forma fundada y motivada la existencia de violaciones y/o incumplimientos a la Ley General y a la presente Ley; o

II. Por denuncia de la persona titular, cuando considere que ha sido afectado por actos del Sujeto obligado, 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 prescribe 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 del cual se tuvo conocimiento.





La verificación no procederá, ni se admitirá en los supuestos de procedencia del recurso de revisión previsto en la presente Ley. Previo a la verificación respectiva, las Autoridades Garantes podrán desarrollar investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respectivo.

**Artículo 110.** Para la presentación de una denuncia no podrán solicitarse mayores requisitos que los que a continuación se describen:

- I. El nombre de la persona que denuncia, o en su caso, de su representante;
- II. El domicilio 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 Sujeto obligado denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación; y
- V. La firma de la persona 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 establezcan las Autoridades Garantes.

Una vez recibida la denuncia, las Autoridades Garantes deberán acusar recibo de la misma. El acuerdo correspondiente se notificará al denunciante.

**Artículo 111.** Las Autoridades Garantes podrán 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 bases de datos de los Sujetos obligados.

Estas medidas sólo podrán tener una finalidad correctiva y serán temporales hasta entonces los Sujetos obligados lleven a cabo las recomendaciones hechas por las Autoridades Garantes.

**Artículo 112.** El procedimiento de verificación concluirá con la resolución que emitan las Autoridades Garantes, dentro de los cincuenta días posteriores a su inicio, en la cual, se establecerán las medidas que deberá adoptar el Sujeto obligado en el plazo que la misma determine.

Cuando en la verificación se advierta que se incurra en una presunta responsabilidad administrativa la Autoridad Garante deberá remitir al órgano interno de control u equivalente de la autoridad competente, la denuncia correspondiente.

## CAPÍTULO SEGUNDO DEL RECURSO DE REVISIÓN





**Artículo 113.** La persona titular, por sí mismo o a través de su representante, podrán interponer un recurso de revisión ante las Autoridades Garantes o la Unidad de Transparencia del Sujeto obligado 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 día siguiente a la fecha de la notificación de la respuesta, a través de los siguientes medios:

I. Por escrito libre en el domicilio de las Autoridades Garantes, según corresponda, o bien, de la Unidad de Transparencia del Sujeto obligado, o en su caso, en las oficinas habilitadas que para el efecto se establezcan;

II. Por correo certificado con acuse de recibo;

III. Por formatos que para el efecto emita las Autoridades Garantes, según corresponda;

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

V. Cualquier otro medio que al efecto establezcan las Autoridades Garantes, según corresponda.

Se presumirá que la persona 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.

En el caso de que el recurso de revisión se interponga ante la Unidad de Transparencia del Sujeto obligado, ésta deberá de remitirlo a las Autoridades Garantes, a más tardar al día siguiente de haberlo recibido.

Cuando el recurso de revisión se presente ante la Unidad de Transparencia del Sujeto obligado o por correo certificado, para el cómputo de los plazos de presentación se tomará la fecha en que las Autoridades Garantes lo reciban.

**Artículo 114.** El recurso de revisión procederá en los siguientes supuestos:

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 Sujeto obligado;

IV. Se entreguen datos personales incompletos;

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

VI. Se niegue el ejercicio de los derechos ARCO de los datos personales;

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. La persona 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 de que fue notificada la procedencia de los mismos; o
- XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO.

**Artículo 115.** Los únicos requisitos exigibles en el escrito de interposición del recurso de revisión serán los siguientes:

- I. El Sujeto obligado ante quien se presentó la solicitud para el ejercicio de los derechos ARCO;
- II. El nombre de la persona titular que recurre o su representante, y en su caso, del tercero interesado, así como el domicilio o medio que señale para recibir notificaciones;
- III. La fecha en que fue notificada la respuesta a la persona titular, o bien, en caso de falta de respuesta, la fecha de la presentación de la solicitud para el ejercicio de los derechos ARCO;
- 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; y
- VI. Los documentos que acrediten la identidad de la persona titular, o en su caso, la personalidad e identidad de su representante. Al recurso de revisión se podrán acompañar las pruebas y demás elementos que la persona titular considere procedentes someter a juicio de las Autoridades Garantes.

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

**Artículo 116.** La persona titular podrá acreditar su identidad a través de cualquiera de los siguientes medios:

- I. Identificación oficial expedida por autoridad nacional;
- II. Firma electrónica avanzada o del instrumento electrónico que la sustituya;
- o
- III. Mecanismos de autenticación autorizados por las Autoridades Garantes, publicados mediante acuerdo general en el Gaceta Oficial de la Ciudad de México.

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



**Artículo 117.** Cuando la persona titular actúe mediante un representante, éste deberá acreditar su personalidad en los siguientes términos:

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 de la persona titular y del representante ante las Autoridades Garantes.

II. Si se trata de una persona moral, mediante instrumento público.

**Artículo 118.** 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.

**Artículo 119.** Si en el escrito de interposición del recurso de revisión la persona titular no cumple con alguno de los requisitos previstos en el artículo 115 de la presente Ley, y las Autoridades Garantes no cuente con elementos para subsanarlos, éste deberá requerir a la persona titular, 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.

La persona titular 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 de 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 tienen las Autoridades Garantes para resolver el recurso, por lo que comenzará a computarse a partir del día siguiente a su desahogo.

**Artículo 120.** Las Autoridades Garantes deberán dictar acuerdo de admisión o de improcedencia dentro de los tres días siguientes a la presentación del recurso de revisión. Admitido el recurso, se integrará un expediente y se notificará al Sujeto obligado, para que, dentro del término de cinco días contados a partir del día siguiente de dicha notificación, produzca su contestación fundada y motivada y aporte las pruebas que considere pertinentes.

**Artículo 121.** En la sustanciación de los recursos de revisión, las partes podrán ofrecer las siguientes pruebas:

- 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; y
- VIII. La presuncional legal y humana.

Las Autoridades Garantes, podrá allegarse de los medios de prueba que considere necesarios, sin más limitación que las establecidas en la Ley.

**Artículo 122.** En la sustanciación del recurso de revisión, las notificaciones que emitan las Autoridades Garantes, surtirán efectos el mismo día en que se practiquen. Las notificaciones podrán efectuarse:

- I. Personalmente en los siguientes casos:
  - 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 del que se trate; y
  - e) En los demás casos que disponga la Ley;
- II. Por correo certificado con acuse de recibo o medios digitales o sistemas autorizados por las Autoridades Garantes y publicados mediante acuerdo general en el Gaceta Oficial de la Ciudad de México, en los casos de la fracción anterior, cuando así lo haya aceptado expresamente la persona promovente;
- 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; o
- V. Por otras formas que autorice la persona recurrente.

**Artículo 123.** Admitido el recurso de revisión, las Autoridades Garantes promoverán la conciliación entre las partes, de conformidad con el siguiente procedimiento:

I. Las Autoridades Garantes, requerirán a las partes a 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 Sujeto obligado 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 determinen las Autoridades Garantes. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.

Queda exceptuada la etapa de conciliación, cuando la persona titular sea niña, niño o adolescente y se haya vulnerado alguno de los derechos contemplados





en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con la Ley, salvo que cuente con representación legal debidamente acreditada;

II. Aceptada la posibilidad de conciliar por ambas partes, las Autoridades Garantes señalarán 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 a que haya recibido la manifestación de la voluntad de conciliar de ambas partes, en la que se procurará avenir los intereses entre la persona titular y el Sujeto obligado.

La persona conciliadora 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. La persona conciliadora podrá suspender cuando lo estime pertinente, o a instancia de ambas partes, la audiencia por una sola ocasión.

En caso de que se suspenda la audiencia, ésta señalará día, hora, y lugar o medio 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 de que el Sujeto obligado o la persona titular o sus respectivos representantes no firmen el acta, 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 de 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 trámite del 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 las Autoridades Garantes, deberán verificar el cumplimiento del acuerdo respectivo; y

VI. El cumplimiento del acuerdo dará por concluido la sustanciación del recurso de revisión, en caso contrario, las Autoridades Garantes aplicarán las medidas de apremio que estime pertinentes para garantizar su cumplimiento. El plazo al que se refiere el artículo 125 de la presente Ley será suspendido durante el periodo de cumplimiento del acuerdo de conciliación.



**Artículo 124.** El cómputo de los plazos señalados en el presente capítulo 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 de las Autoridades Garantes.

**Artículo 125.** Las Autoridades Garantes resolverán 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.

**Artículo 126.** Durante el procedimiento a que se refiere el presente Capítulo, las Autoridades Garantes, deberán aplicar la suplencia de la queja a favor de la persona 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.

**Artículo 127.** Las resoluciones de las Autoridades Garantes podrán:

- I. Sobreseer o desechar el recurso de revisión por improcedente;
- II. Confirmar la respuesta del Sujeto obligado;
- III. Revocar o modificar la respuesta del Sujeto obligado; u
- IV. Ordenar la entrega de los datos personales, en caso de omisión del Sujeto obligado.

Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución.

Los Sujetos obligados deberán informar a las Autoridades Garantes el cumplimiento de sus resoluciones en un plazo de tres días, a partir de que sea cumplimentada dicha resolución.

Cuando las Autoridades Garantes, determinen 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 para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo.

**Artículo 128.** El recurso de revisión podrá ser desechado por improcedente cuando:



- I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 113 de la presente Ley;
  - II. La persona titular, o su representante, no acrediten debidamente su identidad, o la personalidad de este último;
  - III. Las Autoridades Garantes hayan 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 114 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 las Autoridades Garantes, según corresponda;
  - VI. La persona recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos; o
  - VII. La persona recurrente no acredite interés jurídico.
- El desechamiento no implica la prescripción del derecho de la persona titular para interponer ante las Autoridades Garantes, un nuevo recurso de revisión.

**Artículo 129.** El recurso de revisión sólo podrá ser sobreseído cuando:

- I. La persona recurrente se desista expresamente;
- II. La persona recurrente fallezca;
- III. Admitido el recurso de revisión, se actualice alguna causal de improcedencia en los términos de la presente Ley;
- IV. El Sujeto obligado modifique o revoque su respuesta de tal manera que el recurso de revisión quede sin materia; o
- V. Quede sin materia el recurso de revisión.

**Artículo 130.** Las Autoridades Garantes deberán notificar a las partes y publicar las resoluciones, en versión pública, dentro de los dos días siguientes a que se dicten y surtirán efecto al día siguiente de que se efectúen.

**Artículo 131.** La persona titular, el Sujeto obligado o cualquier autoridad deberá atender los requerimientos de información en los plazos y términos que la presente Ley y las Autoridades Garantes establezcan.

**Artículo 132.** Cuando la persona titular, el Sujeto obligado, o cualquier autoridad, se niegue a atender o cumplimentar los requerimientos, solicitudes de información y documentación, emplazamientos, citaciones o diligencias notificadas por las Autoridades Garantes, o facilitar la práctica de las diligencias que hayan sido ordenadas, o entorpezca las actuaciones de las Autoridades Garantes, tendrá por



perdido su derecho para hacerlo valer en algún otro momento del procedimiento y las Autoridades Garantes tendrán por ciertos los hechos materia del procedimiento y resolverá con los elementos que disponga.

**Artículo 133.** Las resoluciones de las Autoridades Garantes serán vinculantes y definitivas para los Sujetos obligados en la vía administrativa.

Los Sujetos obligados deberán cumplir las resoluciones en los plazos y términos establecidos, sin perjuicio de los medios de defensa que procedan conforme a las leyes aplicables.

Las personas titulares de datos personales podrán impugnar las resoluciones de las Autoridades Garantes mediante los recursos y medios de defensa previstos en la Ley de Procedimiento Administrativo de la Ciudad de México, la Ley Orgánica del Tribunal de Justicia Administrativa de la Ciudad de México y la Ley de Amparo, según corresponda.

Ninguna disposición de esta Ley podrá interpretarse en el sentido de limitar el derecho a la tutela jurisdiccional efectiva, el acceso a la justicia o el juicio de amparo reconocidos en los artículos 17 y 103 de la Constitución Política de los Estados Unidos Mexicanos.

## **TÍTULO SEXTO DE LAS MEDIDAS DE APREMIO E INFRACCIONES A LA LEY**

### **CAPÍTULO PRIMERO DE LAS MEDIDAS DE APREMIO**

**Artículo 134.** Para el cumplimiento de las resoluciones y determinaciones emitidas por las Autoridades Garantes, según corresponda, se deberá observar lo dispuesto en el presente Capítulo.

**Artículo 135.** En caso de que no se cumpliera con las resoluciones o determinación, 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 las medidas apremio establecidas en la presente Ley.

Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista al órgano interno de control de las Autoridades Garantes en materia de responsabilidades.

**Artículo 136.** Las Autoridades Garantes podrán imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

- I. La amonestación pública; o



II. La multa, equivalente a la cantidad de 150 hasta 1500 veces el valor diario de la Unidad de Medida y Actualización.

Las multas serán efectivas por conducto de la Secretaría de Finanzas y el monto recaudado se destinará a un fondo para el mejoramiento de la cultura de la transparencia, acceso a la información pública y protección de datos personales, ejecutado por las Autoridades Garantes de acuerdo a su planeación presupuestal.

El incumplimiento de los Sujetos obligados será difundido en los portales de obligaciones de transparencia de las Autoridades Garantes y considerados en las evaluaciones que realicen éstas. En caso de que el incumplimiento de las determinaciones de las Autoridades Garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 143 de 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, sin embargo, para garantizar el cumplimiento, el Sujeto obligado y el servidor público se consideran responsables solidarios, por lo que en caso de que el Sujeto obligado cubra el monto, deberá repetir contra la persona servidora pública responsable.

**Artículo 137.** Para graduar las medidas de apremio establecidas en el presente Capítulo, las Autoridades Garantes deberán considerar:

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

II. La condición económica de la persona infractora; y

III. La reincidencia.

Las Autoridades Garantes establecerán mediante 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.

**Artículo 138.** En caso de reincidencia, las Autoridades Garantes podrán imponer una multa equivalente hasta el doble de la que se hubiera determinado anteriormente.

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





**Artículo 139.** Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio a la persona infractora.

**Artículo 140.** La amonestación pública será impuesta por las Autoridades Garantes y será ejecutada por el superior jerárquico inmediato de la persona infractora con el que se relacione.

**Artículo 141.** Las Autoridades Garantes podrán requerir a la persona infractora la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base en los elementos que se tengan a disposición, entendidos 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 facultadas las Autoridades Garantes para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

**Artículo 142.** En contra de la imposición de medidas de apremio procede el recurso correspondiente ante el Tribunal de Justicia Administrativa de la Ciudad de México.

## CAPÍTULO SEGUNDO DE LAS INFRACCIONES Y SANCIONES

**Artículo 143.** Son causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. 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 de que se trate;

III. Comercializar los datos personales, tales como su uso, transmisión, transferencia, divulgación, difusión, publicación, ocultamiento, alteración, mutilación, distorsión o destrucción que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión, sin el consentimiento de la persona titular;

IV. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, 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;





V. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

VI. Dar tratamiento a sistemas de bases de datos en contravención a los principios y deberes establecidos en la presente Ley;

VII. No contar con el aviso de privacidad, o bien, omitir en el mismo, alguno de sus elementos, de conformidad con lo establecido en la presente Ley y demás disposiciones que resulten aplicables en la materia;

VIII. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las disposiciones jurídicas aplicables. La sanción sólo procederá cuando exista una resolución previa que haya quedado firme, respecto del criterio de clasificación de los datos personales;

IX. Incumplir el deber de confidencialidad establecido en la presente Ley;

X. No establecer las medidas de seguridad en términos de lo dispuesto por la presente Ley;

XI. Presentar vulneraciones a los datos personales por la falta dolosa o negligente en la implementación de medidas de seguridad en términos de lo dispuesto por la presente Ley;

XII. Llevar a cabo la transmisión o transferencia de datos personales, en contravención a lo previsto en la presente Ley;

XIII. Obstruir los actos de verificación de la autoridad;

XIV. Crear bases de datos personales en contravención a lo dispuesto por la presente Ley;

XV. No acatar las resoluciones o determinaciones emitidas por las Autoridades Garantes; y

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

Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos, sin embargo, para garantizar el cumplimiento, el Sujeto obligado y la persona servidora pública se consideran responsables solidarios, por lo que en caso de que el Sujeto obligado cubra el monto, deberá repetir contra la persona servidora pública responsable.

**Artículo 144.** Las causas de responsabilidad previstas en las fracciones VII, X, XIII y XIV del artículo 143, serán sancionadas con apercibimiento público, y en caso de reincidencias, con suspensión del cargo de tres días a tres meses sin goce de sueldo.

**Artículo 145.** Las causas de responsabilidad previstas en las fracciones I, II, IV, V, VI, IX y XI del artículo 143, serán sancionadas con suspensión del cargo de





tres días a tres meses sin goce de sueldo, y en caso de reincidencia, con la destitución de la o las personas responsables.

**Artículo 146.** Las causas de responsabilidad previstas en las fracciones III, XII y XV del artículo 143, serán sancionadas con destitución del cargo y atendiendo a la gravedad de la falta, podrá decretarse la inhabilitación de la persona servidora pública responsable.

**Artículo 147.** Para las causales de responsabilidad a que se refiere el artículo 143, se dará vista a la autoridad competente para que imponga y ejecute la sanción correspondiente.

**Artículo 148.** Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 143 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Las 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, las Autoridades Garantes deberán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que considere pertinentes, en los términos de las leyes aplicables.

**Artículo 149.** En aquellos casos en que la presunta persona infractora tenga la calidad de persona servidora pública, la Autoridad Garante deberá remitir al órgano interno de control de la autoridad competente, la denuncia correspondiente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley, acompañada de un expediente en el que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.

La autoridad que conozca del asunto, deberá informar a la Autoridad Garante, según corresponda de la conclusión del procedimiento, y en su caso, de la ejecución de la sanción.

A efecto de sustanciar el procedimiento citado en este artículo, la Autoridad Garante que corresponda deberá elaborar lo siguiente:

I. Denuncia dirigida al 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; y



II. Expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad, y que acrediten el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La denuncia y el expediente deberán remitirse al órgano interno de control o equivalente, dentro de los quince días siguientes a partir de que la Autoridad Garante tenga conocimiento de los hechos.

**Artículo 150.** La Autoridad Garante deberá denunciar el incumplimiento de las determinaciones que esta emita y que impliquen la presunta comisión de un delito ante la autoridad competente.

## TRANSITORIOS

**PRIMERO.-** El presente Decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

**SEGUNDO.-** Publíquese el presente Decreto en la Gaceta Oficial de la Ciudad de México para su mayor difusión, y en el Diario Oficial de la Federación para conocimiento general.

**TERCERO.-** Las Autoridades Garantes contarán con un plazo de hasta ciento ochenta días naturales, contados a partir de la entrada en vigor del presente Decreto, para emitir y, en su caso, adecuar los acuerdos, lineamientos y normatividad reglamentaria que resulten necesarios para la plena ejecución de la presente Ley, particularmente en materia de derechos ARCO, evaluación de impacto en la protección de datos personales, transferencias y medidas compensatorias.

**CUARTO.-** Se abroga la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, publicada en la Gaceta Oficial de la Ciudad de México, así como las disposiciones reglamentarias y administrativas que se opongan al presente Decreto. Los trámites, procedimientos, recursos y actos administrativos iniciados con anterioridad a la entrada en vigor del presente Decreto se sustanciarán y resolverán conforme a las disposiciones vigentes al momento de su inicio, sin perjuicio del principio pro persona.

**QUINTO.-** Las menciones que en otros ordenamientos jurídicos de la Ciudad de México se hagan al Instituto de Transparencia, Acceso a la Información Pública,



Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, en lo relativo a la materia de protección de datos personales, se entenderán referidas, en lo conducente, al órgano desconcentrado de la Secretaría de la Contraloría General de la Ciudad de México y a las demás Autoridades Garantes en el ámbito de su respectiva competencia.

**SEXO.**- Los recursos humanos, materiales, presupuestales, financieros y tecnológicos del extinto organismo garante local en materia de protección de datos personales se transferirán al órgano desconcentrado de la Secretaría de la Contraloría General de la Ciudad de México y, en su caso, a las autoridades garantes de los demás Poderes y órganos constitucionales autónomos, conforme a los acuerdos de transferencia y a los lineamientos que para tal efecto emita la persona Titular de la Jefatura de Gobierno, garantizando en todo momento el respeto a los derechos laborales adquiridos por las personas servidoras públicas.

**SÉPTIMO.**- La implementación de la presente Ley se sujetará a la disponibilidad presupuestaria que para tal efecto se prevea en el Presupuesto de Egresos de la Ciudad de México para los ejercicios fiscales correspondientes, sin que con ello se autoricen ampliaciones netas al presupuesto autorizado a los Sujetos Obligados, en estricta observancia del principio de austeridad republicana y disciplina financiera previsto en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos.

**OCTAVO.**- Los Sujetos Obligados deberán adecuar sus avisos de privacidad, sistemas de tratamiento de datos personales, documentos de seguridad y procedimientos internos a las disposiciones de la presente Ley dentro de los doscientos cuarenta días naturales siguientes a su entrada en vigor.

**NOVENO.**- Se derogan todas las disposiciones de igual o menor jerarquía que se opongan a la presente Ley.

Dado en el Recinto Legislativo de Donceles, sede del Poder Legislativo de la Ciudad de México el día 19 de mayo del 2026.

**ATENTAMENTE.**

*Andrés Atayde Rubiolo*  
**DIPUTADO ANDRÉS ATAYDE RUBIOL**



III LEGISLATURA

CONGRESO DE LA CIUDAD DE MÉXICO



III LEGISLATURA

Certificado de firma 15/05/2026 11:19

Documento electrónico	Solicitante del proceso de firma Almacenado
<b>Identificador:</b> 6A0754FA9E1C040A92271ABD <b>Nombre y extensión:</b> IDL Ley datos personales.pdf <b>Descripción:</b> <b>Cantidad de páginas:</b> 3 <b>Estado:</b> Firmado <b>Firmantes:</b> 1 <b>Huella digital del contenido del documento original:</b> <small>9ca3a3f2effbcf42839d842fbf42901885240397cd92ea0e606ac62db251bc62</small> <b>Huella digital del contenido del documento firmado:</b> <small>0ab22003afda4e5ad87a3d715922b94766684508989d36b887a2be7a945ae0bd</small>	<b>Nombre:</b> Andrés Atayde Rubiolo <b>Compañía:</b> SR LUZ SA DE CV <b>Correo electrónico:</b> andres.atayde@congresocdmx.gob.mx <b>Teléfono:</b>  <b>Dirección IP:</b> 2806:107e:a:9469:6480:a689:63e3:cca4  <b>Fecha y hora de emisión</b> <b>(America/Mexico_City):</b> 15/05/2026 11:16

Constancia de conservación del documento firmado

Información de la constancia NOM-151	Información del emisor de la constancia NOM-151
<b>Fecha de emisión:</b> 15/05/2026 17:19:05 UTC (15/05/2026 11:19:05 Hora local de la Ciudad de México) <b>Nombre y extensión:</b> <small>c75f2bf0-e3d7-4b24-87e1-35ce2a5f610f.cons</small> <b>Huella digital contenida en la constancia:</b> <small>0ab22003afda4e5ad87a3d715922b94766684508989d36b887a2be7a945ae0bd</small>	<b>Prestador de Servicios de Certificación (PSC):</b> PSC WORLD S.A. DE C.V. <b>Certificado PSC válido desde:</b> 2017-07-19 <b>Certificado PSC válido hasta:</b> 2029-07-19

Firmantes

Firmante 1. Andrés Atayde		
Atributos	Firma	Fecha
<b>Tipo de actuación:</b> Por su Propio <b>Derecho</b> <b>Compañía:</b> <b>Método de notificación:</b> Correo <b>Correo:</b> andres.atayde@congresocdmx.gob.mx <b>Teléfono:</b> <b>Emisor de la firma electrónica:</b> Dibujada en dispositivo <b>Plataforma:</b> <a href="https://app.con-certeza.mx">https://app.con-certeza.mx</a>	ID: 6A0755819E1C040A92271AC0 IP: 2806:107e:a:9469:f089:763:8852:9496  <div style="border: 1px dashed blue; padding: 5px; display: inline-block;"> Firma con texto  <i>Andrés Atayde Rubiolo</i> </div>	<b>Enviado:</b> 15/05/2026 11:18:27 <b>Aceptó Aviso de Privacidad:</b> 15/05/2026 11:18:58 <b>Visto:</b> 15/05/2026 11:18:58 <b>Confirmado:</b> 15/05/2026 11:18:58.441 <b>Firmado:</b> 15/05/2026 11:18:58.442

EL ESPACIO DEBAJO SE HA DEJADO EN BLANCO INTENCIONALMENTE

