P O D E R E J E C U T I V O

SECRETARÍA DE SALUD PÚBLICA DE LA CIUDAD DE MÉXICO

DOCTORA NADINE FLORA GASMAN ZYLBERMANN, SECRETARIA DE SALUD PÚBLICA DE LA CIUDAD DE MÉXICO, con fundamento en los artículos 6, apartado A, fracciones II, III y VIII, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, apartado E, de la Constitución Política de la Ciudad de México; 2, 7, 11, 12, 19 y 24, fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 1, párrafo tercero, 10, 14, 23, fracciones I y II, y 26, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México; 38 y 68, de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México; y

CONSIDERANDO

Que en los artículos 6, apartado A, fracciones II, III y VIII; y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, se establecen las bases en materia de protección de datos personales por parte de los sujetos obligados y el derecho que toda persona tiene a que se efectúe dicha protección.

Que el artículo 7, apartado E, de la Constitución Política de la Ciudad de México, reitera el derecho de privacidad individual y protección de datos personales dentro de la Ciudad de México solo con excepciones expresas en la Constitución Política de los Estados Unidos Mexicanos y las leyes.

Que los artículos 2, 7, 11, 12, 19 y 24, fracción II, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que dicho ordenamiento es la Ley específica en la cual se regula la protección de datos personales y las delimitaciones de su uso, encomendando lo anterior a los sujetos obligados a través de sus facultades.

Que los artículos 1, párrafo tercero, 10, 14, 23, fracciones I y II, y 26, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, limitan el uso de Datos Personales a un fin concreto, lícito y específico, además de establecer el deber a lo sujetos obligados de la Ciudad de México de elaborar políticas y programas de protección de datos personales obligatorios.

Que los artículos 38 y 68, de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, amplían el deber de los sujetos obligados a implementar políticas y programas de protección de datos personales que contengan dirección, operación y control de todos los procesos que impliquen el tratamiento de dichos datos.

Que la protección de datos personales, además de ser un derecho consagrado en distintos ordenamientos, es también un deber legal y moral con el que la Secretaría de Salud Pública de la Ciudad de México se encuentra comprometida.

En virtud a lo anterior, he tenido a bien dictar el siguiente:

ACUERDO POR EL QUE SE CREAN LAS POLÍTICAS INTERNAS DE PROTECCIÓN DE DATOS PERSONALES DE LA SECRETARÍA DE SALUD PÚBLICA DE LA CIUDAD DE MÉXICO

ÍNDICE

CAPÍTULO I.
DISPOSICIONES GENERALES

1. CONSIDERACIONES

El derecho a la protección de datos personales es un derecho humano reconocido por el artículo 6 y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, del cual gozan todas las personas para decidir sobre el uso y manejo de su información personal, y el cual establece obligaciones de los particulares y de las instituciones públicas que tratan datos personales y otorga derechos a los titulares de los datos, a fin de garantizar el buen uso de los mismos y el respeto a su privacidad, así como el derecho de las personas para decidir, de manera libre e informada, sobre el uso de su información personal.

Los datos personales son cualquier información relativa a una persona física, que la identifica o hace identificable, es la información que la describe, que le da identidad, la caracteriza y diferencia de otros individuos.

El titular de los datos personales, es el dueño de los mismos, aun cuando éstos se encuentren en posesión de un tercero para su tratamiento, la Secretaría de Salud Pública de la Ciudad de México (Secretaría) como una Dependencia de la Administración Pública Centralizada, tiene la obligación de proteger los datos personales que obren en sus archivos y sobre los cuales efectúe algún tipo de tratamiento.

Por lo anterior, la Secretaría, es la responsable de su debido resguardo y tratamiento de los Datos Personales recabados, así como de aquellos que obren en su poder conforme a sus atribuciones, garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como con los deberes de seguridad y confidencialidad.

Para cumplir con las anteriores responsabilidades, la Secretaría, debe adoptar mecanismos acordes con la normatividad en materia de protección de datos personales, como son la elaboración de políticas y programas de protección de los mismos, obligatorias y exigibles al interior de la Dependencia.

2. OBJETIVO

El objetivo de las presentes **Políticas Internas de Protección de Datos Personales** es establecer los criterios generales de actuación en materia de protección de datos personales, que se encuentren bajo resguardo de la Secretaría, a fin de proteger los datos personales de los ciudadanos y garantizar su privacidad.

3. ALCANCE

El presente documento es de observancia general y obligatoria para todas las personas que laboran en las unidades administrativas que integran la Secretaría, conforme a sus atribuciones.

4. APLICACIÓN

Las presentes políticas, serán aplicables a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos de esta Secretaría, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

5. GLOSARIO

Para los efectos de las presentes Políticas, además de las definiciones previstas en la normativa en la materia, se entenderá por:

Administrador: Responsable de gestionar y proteger los activos de una organización, garantiza la calidad, integridad y seguridad de los datos mediante la implementación y el cumplimiento de políticas y procedimientos de gobernanza de datos.

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

Base de datos: Conjunto ordenado de datos personales referentes a una persona identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procedimiento, almacenamiento y organización.

Bloqueo: 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 en la base de datos que corresponda.

Comité de Transparencia: Órgano Colegiado e instancia a la que hace referencia el artículo 39, de la Ley General de Transparencia y Acceso a la Información Pública, y 88, de la Ley de Transparencia y Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, y la máxima autoridad en materia de protección de datos personales al interior del sujeto obligado.

Consentimiento: Toda manifestación previa, de voluntad libre, específica e informada e inequívoca por la que el titular acepta, mediante declaración o acción afirmativa, el tratamiento de los datos personales.

Datos personales: Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

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

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

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

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

Encargado: Persona física o jurídica pública o privada, ajena a la organización del Responsable, que sola o conjuntamente con otros trate los datos personales a nombre y por cuenta del responsable.

Finalidad: Los datos personales y recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

GOCDMX: Gaceta Oficial de la Ciudad de México.

Lineamientos: Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

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

LPDPPSOCDMX: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la CDMX.

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

Responsable del tratamiento de datos personales: El Sujeto Obligado que posee los datos personales de particulares.

RESDP: Registro Electrónico de Sistemas de Datos Personales

Secretaría: Secretaría de Salud Pública de la Ciudad de México.

Sujeto Obligado: Autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal o de las demarcaciones territoriales de la Ciudad de México.

Sistema de Datos Personales (SDP): Conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera que sea su forma o modalidad de su creación, almacenamiento organización y acceso.

Supresión: Baja archivística de los datos personales conforme a las disposiciones jurídicas aplicables en materia de archivos, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Titular: Persona física a quien corresponden los datos personales.

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

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, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 41, de la Ley General de Transparencia y Acceso a la Información Pública; 92, de la Ley de Transparencia y Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, así como 1, párrafo tercero,10, 14, 23, fracciones I y II, 26, fracción I, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a os datos y/o a los sistemas de datos personales.

Vulneración: Pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

6. MARCO NORMATIVO

Constitución

* Constitución Política de los Estados Unidos Mexicanos;
* Constitución Política de la Ciudad de México;

Leyes

* Ley General de Transparencia y Acceso a la Información Pública;
* Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

* Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;
* Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México; y
* Ley de Archivos de la Ciudad de México.

Lineamientos

* Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Normativa Archivística

* Catálogo de Disposición Documental: regula plazos de conservación y baja documental.

Guía para el Borrado Seguro de Datos Personales del INAI

* Define métodos seguros de destrucción física y electrónica y exige trazabilidad.

CAPÍTULO II.
PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

De conformidad con lo establecido por el artículo 10, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados **(LGDPDPSO) DOF 20-03-2025,** y el 9, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados **(LPDPPSOCDMX),** el tratamiento de datos personales son reglas fundamentales que rigen la forma en que todo responsable debe manejarlo, buscando garantizar la protección de la privacidad y los derechos de los individuos, estos principios son: **licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, responsabilidad, confidencialidad, transparencia y temporalidad** para el tratamiento de datos personales, mismos que se detallan a continuación:

Principio	Definición
1. Licitud	El tratamiento debe realizarse conforme a las atribuciones legales del responsable, con base en la normativa aplicable.
2. Finalidad	El tratamiento debe estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones del responsable. Incluirá el ciclo de vida del dato personal, de tal manera que concluida ésta, los datos puedan ser suprimidos, cancelados o destruidos
3. Lealtad	Prohíbe obtener o tratar datos personales mediante medios engañosos o fraudulentos, privilegiando los intereses del titular.
4. Consentimiento	El responsable debe solicitar autorización del titular para tratar sus datos, especialmente si son sensibles. Puede ser expreso o tácito, según el caso.
5. Calidad	Los datos deben ser exactos, completos, pertinentes, correctos y actualizados para cumplir con la finalidad del tratamiento.
6. Proporcionalidad	Sólo deben recabarse los datos personales que resulten estrictamente necesarios, adecuados y relevantes para la finalidad.
7. Información	El titular debe conocer el uso que se dará a sus datos, mediante un aviso de privacidad claro y accesible, antes de ser recabados.
8. Responsabilidad	El responsable debe adoptar medidas necesarias para garantizar el cumplimiento de los principios, deberes y derechos establecidos en la ley.
9. Confidencialidad	El responsable garantizará la secrecía y la difusión de los datos. Sólo la persona titular podrá autorizar la difusión de los mismos.

10. Transparencia	La información relacionada con el tratamiento de datos será accesible y fácil de entender, y siempre a disposición de la persona titular.
11. Temporalidad	Los datos personales tendrán un ciclo de vida o una temporalidad vinculada a la finalidad para la cual fueron recabados y tratados y una vez concluida esta finalidad, pueden ser destruidos, cancelados o suprimidos

CAPÍTULO III.
COMITÉ DE TRANSPARENCIA

Los Comités de Transparencia son órganos colegiados, integrados de manera democrática en los entes públicos. En materia de protección de datos personales, constituyen el órgano responsable de coordinar, supervisar y validar las acciones institucionales que garanticen el cumplimiento de la legislación aplicable. Su actuación se rige por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, y demás disposiciones normativas.

ATRIBUCIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES
Conforme los artículos,78, de la LGPDPPSO y 75, de la LPDPPSOCDMX, el Comité de Transparencia tiene, entre otras, las siguientes atribuciones:

a) Coordinar y supervisar las acciones necesarias para garantizar el ejercicio del derecho a la protección de datos personales dentro del Sujeto Obligado.
b) Instituir procedimientos internos para la atención eficiente de solicitudes de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).
c) Establecer criterios específicos para la observancia de la normativa aplicable en materia de protección de datos personales.
d) Supervisar el cumplimiento de lo estipulado en los documentos de seguridad.
g) Confirmar, modificar o revocar la clasificación de información como confidencial o reservada, cuando se trate de datos personales.
i) Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales, y
j) 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 responsables.

Las decisiones del Comité deben registrarse mediante actas debidamente firmadas por sus integrantes. Toda resolución en materia de datos personales debe notificarse a las unidades administrativas responsables del tratamiento, y conservarse como parte del expediente institucional.

CAPÍTULO IV.
FINALIDAD Y TRATAMIENTO DE DATOS PERSONALES

La finalidad es el propósito específico, lícito, explícito y legítimo por el cual se recaban y utilizan los datos personales. Todo tratamiento debe estar vinculado directamente con las atribuciones legales del Sujeto Obligado.

1. CONFIDENCIALIDAD DE LAS PERSONAS TRABAJADORAS DE LA SECRETARÍA DE SALUD PÚBLICA DE LA CIUDAD DE MÉXICO.

a) Los datos personales recabados y tratados por la Secretaría, en el ejercicio de sus atribuciones, deberán ser protegidos en términos de la normativa contenida en las presentes Políticas y aquella que resulte aplicable.

b) Toda persona que labore en la Secretaría, firmará un documento de confidencialidad en el cual se compromete a proteger, resguardar y tomar las medidas de seguridad necesarias para la protección de la información institucional que

resguarde conforme a sus atribuciones, y de forma especial, aquella que contenga datos personales (Anexo I Formato Carta de confidencialidad).

2. ESPECIFICACIONES DEL TRATAMIENTO DE DATOS PERSONALES

De conformidad con el artículo 10, de la LPDPPSOCDMX, en correlación con el 8, de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, todo tratamiento de datos personales que efectúe el responsable deberá sujetarse a los principios, facultades o atribuciones, además de estar justificado por finalidades concretas, lícitas, explícitas y legítimas detalladas a continuación:

a) Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en la persona titular;
b) Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;
c) Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable; y
d) Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento de la persona titular.

3. OBTENCIÓN DE DATOS PERSONALES

a) Las unidades administrativas sólo podrán recabar datos personales conforme a las atribuciones, facultades y competencias que les confiere la normativa aplicable.
b) Las personas que recaben datos personales de forma directa, deberán estar plenamente identificadas ante los titulares de los mismos.
c) Las personas que recaben datos personales deberán asegurarse de contar previamente con el consentimiento de la persona titular, a través del aviso de privacidad respectivo.
d) Tratándose de datos personales sensibles, las personas que los tratan deberán asegurarse de que el consentimiento de la persona titular sea expreso.
e) De ninguna manera deben transmitirse los datos personales recabados por correo electrónico o cualquier otro medio digital.
f) No deberá usarse papel reciclado que contenga datos personales.

4. FINALIDAD

El tratamiento debe estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones del responsable.

5. TRANSFERENCIAS DE DATOS PERSONALES

La transferencia es toda comunicación de datos personales dentro y fuera del territorio mexicano, realizada a personas distintitas del titular, al responsable o al encargado y cumplan con los siguientes requisitos:

a) Siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles y análogas con la finalidad que motivó el tratamiento inicial de los datos personales, y en estricta observancia a los preceptos contenidos en la Ley y Lineamientos. Las transferencias a otras instituciones siempre deberán estar contenidas en el aviso de privacidad respectivo.

b) Únicamente se deben transferir los datos personales a los sujetos obligados a nivel local y federal que estén establecidos en el Acuerdo de Creación o de Modificación, conforme a las finalidades que la justifican.

Por otra parte, cuando se remita información que contenga datos personales al interior de la dependencia, entre las unidades administrativas, se deberá comunicar por escrito, que la información corresponde a datos personales, así como especificar las finalidades para las cuales se realiza la entrega y la obligación que la persona servidora pública tiene de guardar confidencialidad y protección de los mismos.

Otras medidas de seguridad, cuando se remitan datos personales entre unidades administrativas son:

a) Nunca deberán transferirse datos personales por correo electrónico o cualquier otro medio digital.

b) La entrega de la información con datos personales deberá hacerse en una memoria electrónica o cualquier dispositivo digital de persona a persona, mediante un escrito libre en el que señale que se entregan datos personales y que el receptor deberá guardar las medidas de seguridad que considere pertinentes para su debida protección.

6. EJERCICIO DE DERECHOS ARCO

a) Cuando una unidad administrativa reciba una solicitud de Derechos ARCO, previamente la Unidad de Transparencia debió haber acreditado la titularidad o representación del solicitante. Para brindar respuesta, las áreas deben observar el "Procedimiento para garantizar el derecho de acceso a la información pública y a la protección de datos personales de la Secretaría de Salud Pública de la Ciudad de México".

b) La información que contiene datos personales sólo podrá ser entregada a su titular o representante acreditado ante la Unidad de Transparencia, siendo ésta la única instancia autorizada para la entrega de datos personales de manera presencial a la persona solicitante.

c) La entrega de datos personales a su titular o representante nunca se llevará a cabo de manera electrónica.

7. CORREOS ELECTRÓNICOS QUE CONTENGAN DATOS PERSONALES

a) Cuando se presente una solicitud de acceso a la información pública o una solicitud de Derechos ARCO, que involucre correos electrónicos que contengan datos personales, las unidades administrativas deberán elaborar las versiones públicas respectivas.

b) Si una unidad administrativa recibe algún correo electrónico de particular, empleado, proveedor o persona física o moral que contenga datos personales, deberá resguardarlos y protegerlos; así como analizar el contenido para determinar si se trata de un trámite administrativo, una petición, una queja, una consulta, una solicitud de Derechos ARCO, y darle el tratamiento respectivo. En dicho análisis podrá asesorarse con la Unidad de Transparencia.

c) Los correos electrónicos y teléfonos que utilicen las personas servidoras públicas de la Secretaría, en sus comunicaciones oficiales, ya sea por medio impreso o electrónico, deberán ser los institucionales.

CAPÍTULO V.
SUPRESIÓN, ELIMINACIÓN O BORRADO DE DATOS PERSONALES

La supresión, eliminación o borrado de los datos personales, se realizará una vez que hayan cumplido la finalidad de la recabación de los mismos y conforme al ciclo de vida archivístico establecido en el Catálogo de Disposición Documental de la Dependencia.

La conservación de los datos personales o Sistemas de Datos Personales no deberá exceder 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.

El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales o Sistemas de Datos Personales que lleve a cabo, en los cuales se incluya el ciclo de vida vinculado a la finalidad de los mismos, de conformidad con lo dispuesto en la Ley.

Lo anterior aplica a todas las unidades administrativas de la Secretaría que realicen tratamiento de datos personales, tanto en medios físicos como electrónicos, en el marco de sus atribuciones.

1. NORMATIVIDAD

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, Ley de Archivos de la Ciudad de México, Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, Catálogo de Disposición Documental de la Secretaría y Guía para el Borrado Seguro de Datos Personales del INAI.

2. PRINCIPIOS APLICABLES

a) Finalidad: Conservación limitada al cumplimiento de la finalidad original.
b) Temporalidad: Supresión posterior al vencimiento del plazo legal o documental.
c) Seguridad: Eliminación bajo medidas que garanticen confidencialidad e irreversibilidad.
d) Responsabilidad: Documentación y trazabilidad del proceso por parte del responsable del tratamiento.

3. PROCEDIMIENTO OPERATIVO

a) Conservación:

I. Los datos personales se conservarán conforme al ciclo de vida documental establecido en el Catálogo de Disposición Documental de la Secretaría.
II. Se considerarán aspectos administrativos, médicos, contables, fiscales, jurídicos e históricos.

b) Bloqueo: Antes de la supresión, los datos podrán ser bloqueados para evitar su uso, salvo por requerimientos legales o auditorías.

c) Supresión y Eliminación: La eliminación debe ser irreversible, segura y ambientalmente responsable.

I. Métodos físicos: trituración, incineración, destrucción química.
II. Métodos electrónicos: sobreescritura, destrucción de discos, borrado seguro.
III. Evidencia documental: actas, certificados, fotografías, bitácoras.

4. RESPONSABLES

Rol	Función
Responsable del Tratamiento	Ejecuta y documenta el proceso de supresión.
Unidad Administrativa	Aplica los métodos de eliminación.
Comité de Transparencia	Supervisa la correcta supresión conforme al artículo 78, fracciones I y V, de la LGPDPPSO, en correlación con el 75, de la LPDPPSOCDMX

5. REVISIÓN PERIÓDICA

a) Cada unidad administrativa deberá realizar una revisión anual del ciclo de vida de los datos personales y de los sistemas que los contienen.
b) Se verificará el cumplimiento de los plazos de conservación y la ejecución de la supresión.

6. REFERENCIAS TÉCNICAS

a) Se podrá utilizar la Guía para el Borrado Seguro de Datos Personales del INAI como referencia técnica.
b) Se recomienda establecer formatos estandarizados para actas de destrucción, certificados y bitácoras.

7. MEDIDAS DE SEGURIDAD
El procedimiento de eliminación debe cumplir con:

a) Irreversibilidad
b) Confidencialidad y seguridad
c) Sostenibilidad ambiental

8. CUADRO INTEGRAL DE SUPRESIÓN Y ELIMINACIÓN DE DATOS PERSONALES

Categoría	Elemento	Descripción / Detalle
Fundamento Jurídico	LGPDPPSO	Art. 16, 18, 23, 24, 78, fracciones I y V: establecen principios de finalidad, temporalidad, seguridad y supervisión por el Comité de Transparencia.
	Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México	Art. 113 permiten subcontratación
	Guía	Define métodos seguros de destrucción física y electrónica, y exige trazabilidad.
	Normativa Archivística	Catálogo de Disposición Documental: regula plazos de conservación y baja documental.
Subcontratación	Definición	Delegación a un tercero (Encargado) para ejecutar el borrado seguro bajo contrato.
	Fundamento	LPDPPSOCDMX, artículos 57 y 58, y Lineamientos, art. 113. Debe garantizar medidas de seguridad y evidencia.
	Evidencia	Actas, certificados, fotografías, bitácoras.
Medios Físicos	Trituración	Económica, puede hacerse internamente. Requiere evidencia documental.
	Incineración	Irrecuperable, pero contaminante y peligrosa. Requiere evidencia.
	Químicos	Irrecuperable, pero contaminante y peligrosa. Requiere evidencia.
Medios Electrónicos	Sobreescritura	Reemplaza datos con patrones. Económica, requiere software especializado.
	Desmagnetización	Elimina campo magnético. Rápida, no aplica a SSD.
	Destrucción física	Romper o triturar el dispositivo. Irrecuperable, requiere manejo de residuos.
	Borrado criptográfico	Elimina claves de cifrado. Rápido, depende de robustez del cifrado.
Evidencia Documental	Requisitos	Actas, certificados, fotografías, bitácoras. Deben demostrar cumplimiento normativo.
Medidas de Seguridad	Irreversibilidad	El método debe impedir recuperación.
	Confidencialidad	Debe proteger los datos durante el proceso.
	Sostenibilidad	Preferir métodos con bajo impacto ambiental.
Supervisión	Comité de Transparencia	Responsable de vigilar la supresión conforme a la ley.

9. RECOMENDACIONES OPERATIVAS

a) Documentar el proceso: Actas, bitácoras, certificados y evidencia fotográfica.
b) Evaluar el tipo de medio: SSD, HDD, USB, servidores, etc.
c) Evitar métodos reversibles: El simple “formateo rápido” no es seguro.
d) Subcontratación: Si se contrata a un tercero, debe garantizar la eliminación segura y entregar evidencia del proceso.

El Comité de Transparencia es responsable de supervisar la supresión de los datos personales, conforme lo dispuesto por el artículo 78, fracciones I y V, de la LGPDPPSO, y 75, de la LPDPPSOCDMX.

CAPÍTULO VI
SISTEMAS DE DATOS PERSONALES

La Secretaría de Salud Pública de la Ciudad de México, es la Responsable de los SDP, y es a través de las personas titulares de sus Direcciones Generales y Direcciones Administrativas, quienes determinarán la creación, modificación o supresión de SDP, cuando derivado de la normativa aplicable y de sus atribuciones, recaben y traten datos personales previo al inicio de una actividad o acción que realice la Dependencia.

La creación, modificación o supresión de un SDP, se realiza mediante la emisión del Acuerdo respectivo, el cual debe ser publicado en la GOCDMX.

1.- ACUERDO DE CREACIÓN DE UN SISTEMA DE DATOS PERSONALES

El Acuerdo de Creación debe publicarse en la GOCDMX, previo a la recabación y tratamiento de datos personales, por lo que la unidad administrativa, con anticipación deberá solicitar mediante oficio a la Unidad de Transparencia la creación de un SDP, por lo que se le solicitará a la persona Responsable del SDP, la siguiente información para elaborar el Acuerdo de creación de un Sistema de Datos Personales:

a. Finalidad y usos previstos de los datos personales a tratar.
b. Normativa aplicable que faculta a la Secretaría a recabar los datos personales.
c. Los Sujetos Obligados a los que se pueden realizar transferencias.
d. Personas físicas o grupos de las personas sobre las que se recaben o traten los datos personales
e. Los datos identificativos, electrónicos, académicos u otra categoría de datos que van a recabar.
f. El Modo de tratamiento, si es físico, automatizado o mixto.
g. La persona Responsable, en este caso el nombre del Sujeto obligado, mediante la unidad administrativa facultada.
h. Los cargos de las personas usuarias quienes tendrán acceso al tratamiento de los datos recabados.
i. Encargados, si es el caso, que es una persona física o jurídica pública o privada, ajena a la organización del Responsable, que sola o conjuntamente con otros trate los datos personales a nombre y por cuenta del responsable.
j. El nivel de seguridad, que puedes ser: básico, medio o alto.
k. Medidas de seguridad: si son administrativas, físicas y /o técnicas, o todas las anteriores.

1. Una vez elaborado el Acuerdo de Creación del SDP, pasará a revisión del área jurídica de la Dependencia para su posterior publicación en la GOCDMX
2. Una vez publicado el Acuerdo de Creación en la GOCDMX, se elaboran los avisos de privacidad (Simplificado e Integral) mismos que deben ser publicados en el Micrositio de Transparencia de la Secretaría.
3. Posteriormente o a la par, se elabora el Documento de Seguridad, el cual es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la persona responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.
4. Una vez publicado el Acuerdo en la Gaceta Oficial, se deberá ingresar en el Registro Electrónico de Sistema de Datos Personales (RESDP), plataforma administrada por el Órgano Garante.

2.-ACUERDO DE MODIFICACIÓN DE UN SISTEMA DE DATOS PERSONALES

La modificación de un SDP es la acción de cambiar o actualizar los diversos elementos que componen un SDP existente. Surge cuando se presenta un cambio que afecta la integración o tratamiento del SDP.

El Acuerdo de Modificación del SDP tiene el mismo proceso de publicación y debe indicar qué apartados del documento han sido modificados.

3.-ACUERDO DE SUPRESIÓN DE UN SISTEMA DE DATOS PERSONALES

Este documento se elabora en los siguientes supuestos:

a. Se haya cumplido la finalidad y/o ciclo de vida de los datos personales, en este caso se deberá también atender a lo que disponga el Catálogo de Disposición Documental.
b. Que el responsable ya no cuenta con la facultad o atribución para realizar el tratamiento de datos, es decir que, por reforma a la normativa aplicable o por la extinción del sujeto obligado se deje de tener la atribución para tratar los datos personales, relacionada con la finalidad del sistema.
c. Que no existe una previsión expresa en la Ley aplicable que exija su conservación.

Antes de realizar la supresión del sistema de datos personales, se debe someter ante el Comité Técnico Interno de Administración de Documentos (COTECIAD) la baja documental de la información que integre dicho sistema y que dicho órgano emita el acta respectiva.

La supresión de un Sistema de Datos Personales implica la eliminación o borrado del sistema, considerando las medidas previamente establecidas para el soporte documental.

CAPÍTULO VII.
DOCUMENTO DE SEGURIDAD

El objeto de este instrumento es garantizar que todo tratamiento de datos personales cuente con las medidas de seguridad para la protección de datos personales y las obligaciones previstas en la LPDPPSOCDMX y su finalidad es que el sujeto obligado cumpla con el tratamiento lícito, seguro y responsable de los datos personales.

El Documento de Seguridad es elaborado por el Responsable del SDP, quien a su vez designará mediante oficio al Responsable de Seguridad del citado documento, en el cual debe enunciar sus funciones y obligaciones.

ELEMENTOS DEL DOCUMENTO DE SEGURIDAD

Una de las particularidades que contempla la legislación en materia de datos personales a nivel local respecto al documento de seguridad, es que se deben señalar los datos generales del Sistema de Datos Personales, es decir, se tiene describir la formalización de la acción que involucra el tratamiento de datos personales, de la siguiente manera:

a. Nombre del sistema que debe coincidir con el publicado en la GOCDMX.
b. Fecha de publicación en la GOCDMX, indicar la fecha de la creación del SDP.
c. Fecha de Inscripción en el RESDP
d. Folio de inscripción en el RESDP, que arroja el acuse cuando se registra en el Sistema.

Los elementos mínimos que debe contener el Documento de Seguridad, son:

I. Datos generales del sistema de datos personales
II. Inventario de datos personales
III. Funciones y obligaciones de las personas que intervienen en el tratamiento de los datos personales: responsable y usuarios
IV. Registro de incidencias
V. Mecanismos de Identificación y autentificación
VI. Control de acceso, gestión de soportes y copias de respaldo y recuperación
VII. Análisis de riesgo
VIII. Análisis de brecha
IX. Responsable de seguridad
X. Registro de acceso
XI. Mecanismos de monitoreo y revisión de las medidas de seguridad
XII. Plan de trabajo
XIII. Programa general de capacitación

Con este Documento se busca contribuir al mejoramiento de las prácticas en el tratamiento y evitar el daño, pérdida, alteración, destrucción, uso, acceso o cualquier tipo de vulneración de los datos personales con los que cuenta el Sujeto

Obligado, derivado de la información que poseen de las personas físicas a las cuales prestan, dan o reciben un servicio y de las personas que laboran en ellas, a fin de hacer eficiente sus procesos y ser expeditos en sus respuestas.

Este instrumento es confidencial y debe estar resguardado por el Responsable del Sistema de Datos Personales y únicamente tendrá acceso la persona Responsable de Seguridad.

CAPÍTULO VIII
AVISO DE PRIVACIDAD

Las personas titulares de las unidades administrativas de la Secretaría que recaben datos personales serán responsables de la elaboración y la difusión del aviso de privacidad, en el cual se informe a los titulares, previo al tratamiento de sus datos personales: cuáles serán los datos a tratar, identificando aquellos que sean sensibles; las finalidades del tratamiento; en su caso, si éstos serán transferidos especificando a quién y para qué fin; los medios y procedimientos para ejercer los Derechos ARCO; en suma, las características principales del tratamiento.

Las unidades administrativas de la Secretaría son responsables de identificar aquellos procesos internos en los cuales se recaban datos personales, a fin de que antes de su obtención, notifiquen a la Unidad de Transparencia, para la elaboración de Acuerdo de Creación de un Sistema de Datos Personales y la subsecuente elaboración de los avisos de privacidad y el Documento de Seguridad.

Cuando los datos son obtenidos por cualquier medio electrónico, óptico, sonoro, visual o a través de cualquier otra tecnología, el aviso de privacidad debe ser puesto a disposición en lugar visible, considerando los medios o mecanismos para que se conozca el texto completo del aviso y deberá contener al menos, la siguiente información:

1. OBJETIVO DEL AVISO DE PRIVACIDAD

El aviso de privacidad tiene por objeto informar a la persona titular sobre la finalidad y tratamiento a que serán sometidos sus datos personales, a fin de que esté en posibilidad de tomar decisiones informadas sobre el uso de éstos y, en consecuencia, mantener el control y disposición de los mismos. Así también darle a conocer cómo puede ejercer su derecho a la protección de los datos personales (ARCO).

2. CARACTERÍSTICAS DEL AVISO DE PRIVACIDAD

Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, debe estar redactado y estructurado con un lenguaje sencillo, claro y comprensible, que facilite su entendimiento, para lo cual deberá atender al perfil de los titulares a quienes será dirigido, con la finalidad de que sea un mecanismo de información práctico y eficiente.

3. MODALIDADES DE AVISO DE PRIVACIDAD

El aviso de privacidad se pondrá a disposición del titular de los datos personales en dos modalidades, Simplificado e Integral:

AVISO DE PRIVACIDAD SIMPLIFICADO deberá contener lo siguiente:

Contenido	Descripción
Denominación del responsable	Secretaría de Salud Pública de la Ciudad de México.
Nombre del Sistema de Datos Personales (SDP)	De acuerdo a la Publicación del Acuerdo de Creación del SDP.
Finalidades del Tratamiento para las cuales se recaban los datos personales	Las finalidades u objetivos por los que se requiere recabar y tratar los datos personales.
Transferencias de los datos personales que requieran consentimiento	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 los datos personales, conforme a la

	normativa.
Los mecanismos y medios disponibles para que el titular ejerza los Derechos ARCO	Plataforma Nacional de Transparencia, en la Unidad de Transparencia y por correo electrónico institucional de la Unidad de Transparencia.
Domicilio de la Unidad de Transparencia	Av. Insurgentes Norte 423, Planta Baja, Col. Nonoalco Tlatelolco, Alcaldía Cuauhtémoc, Ciudad de México.
Sitio donde podrá consultar el aviso de privacidad integral	Micrositio de Transparencia de la Secretaría.

AVISO DE PRIVACIDAD INTEGRAL deberá contener:

Contenido	Descripción
El domicilio del responsable	Av. Insurgentes Norte 423, Planta Baja, Col. Nonoalco Tlatelolco, Alcaldía Cuauhtémoc, Ciudad de México.
Los datos personales que serán sometidos a tratamiento	Enumerar cada uno de los datos personales, señalando aquéllos que sean sensibles.
Fundamento legal	Normativa interna y/o externa que faculte a la unidad administrativa al tratamiento.
Finalidades	Las finalidades u objetivos por los que se requiere tratar los datos personales.
Los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO	Plataforma Nacional de Transparencia, en la Unidad de Transparencia y por correo electrónico institucional de la Unidad de Transparencia.
El domicilio de la Unidad de Transparencia	Av. Insurgentes Norte 423, Planta Baja, Col. Nonoalco Tlatelolco, Alcaldía Cuauhtémoc, Ciudad de México.
Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad	Micrositio de Transparencia de la Secretaría.

La Unidad de Transparencia debe revisar y validar el contenido de los avisos de privacidad integral y simplificado que elabore cada unidad administrativa, y una vez que sea revisado y cumpla con los requerimientos de ley, podrá ser publicado en el Micrositio de la Secretaría.

Los avisos de privacidad serán publicados en el Micrositio de la Secretaría; sin menoscabo de que sean utilizados por las unidades administrativas generadoras para difundirlos en medios impresos, plataformas tecnológicas, o cualquier medio que sea de utilidad para los particulares.

Cuando un aviso de privacidad requiera alguna modificación, la unidad administrativa elaborará la versión actualizada y la enviará para su revisión, autorización y publicación, a la Unidad de Transparencia.

4. DIFUSIÓN DEL AVISO DE PRIVACIDAD HACIA LOS TITULARES

Cuando la obtención de datos personales sea presencial, el Aviso de Privacidad Simplificado deberá colocarse en un lugar visible y accesible y hacerlo del conocimiento del titular.

Cuando la obtención de datos personales sea por medio de una plataforma digital para tal efecto, o similar, el Aviso de Privacidad Simplificado, deberá mostrarse en la pantalla de la misma, en un lugar visible y contar con un mecanismo para que el titular otorgue el consentimiento expreso cuando así se requiera.

Cuando la obtención de datos personales sea mediante una llamada telefónica, el conmutador de la Secretaría, cuenta con una grabación del aviso de privacidad que protege sus datos personales.

CAPÍTULO IX.
MEDIDAS DE SEGURIDAD

Las medidas de seguridad comprenden el conjunto de acciones, actividades, controles y mecanismos administrativos, técnicos y físicos implementados por los sujetos obligados, con el propósito de proteger los datos personales y los sistemas que los contienen frente a posibles daños, pérdidas, alteraciones, accesos, usos o transmisiones no autorizadas.

En ese sentido, se recomienda al personal que interviene en el tratamiento de datos personales adoptar, entre otras, las siguientes medidas:

a) Establecer controles de acceso físico a los SDP.
b) Utilizar contraseñas robustas y renovarlas periódicamente.
c) Evitar compartir credenciales de acceso entre personas usuarias.
d) Resguardar expedientes físicos en espacios cerrados y bajo llave.
e) Cifrar la información sensible en medios electrónicos.
f) Realizar respaldos periódicos de la información.
g) Capacitar al personal en materia de protección de datos personales.
h) Reportar de inmediato cualquier incidente de seguridad a la Unidad de Transparencia.

Estas medidas deben ser proporcionales al tipo de datos tratados y al nivel de riesgo asociado, y deben revisarse y actualizarse periódicamente para garantizar su eficacia.

Algunas medidas que se sugiere al personal que trata datos personales son:

a) Las personas servidoras públicas de la Secretaría, que con motivo de sus funciones, cargo o comisión tengan acceso a datos personales, no podrán reproducirlos ni difundirlos mediante ningún medio, sea físico o electrónico, a menos que sea necesario para el ejercicio de sus funciones.

b) Las unidades administrativas deberán contar con un inventario de bases de datos que contengan datos personales y designar a una persona que sean responsables del tratamiento y protección de dichas bases de datos (administradores y usuarios).

c) Las personas que, con motivo de su empleo, cargo o comisión, tengan acceso a datos personales contenidos en medios electrónicos, deberán contar con contraseñas seguras, las cuales no podrán ser compartidas con terceros.

d) Las personas que por sus funciones en la Dependencia tengan documentos que contengan datos personales, deberán tener el adecuado resguardo de éstos, con medidas de seguridad físicas o administrativas.

e) Las unidades administrativas deberán establecer medidas de seguridad generales, físicas, administrativas y técnicas para la protección de la información que contenga datos personales.

f) Los datos personales deberán ser tratados con confidencialidad, entendiéndose como la obligación de secreto, discreción y custodia que incumbe a toda persona que maneja, usa, recaba, utiliza o transfiere datos personales, es decir, no podrán difundirse ni compartirse con terceros salvo que exista consentimiento para ello o alguna obligación normativa que requiera su difusión.

1. MEDIDAS DE SEGURIDAD FÍSICAS, ADMINISTRATIVAS Y TÉCNICAS

De manera enunciativa más no limitativa, entre las medidas de seguridad físicas, administrativas y técnicas que se recomienda:

a) Identificación, clasificación y borrado seguro de la información.
b) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea únicamente con usuarios identificados y autorizados.
c) Generar un esquema de seguridad para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

d) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
e) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales
f) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
g) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.
h) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
i) El Documento de seguridad es de carácter confidencial, por lo que representa un documento que debe resguardarse bajo las más altas medidas de seguridad.

2. VULNERACIÓN A LA SEGURIDAD DE LOS DATOS PERSONALES

La vulneración tiene lugar cuando, intencionada o no intencionadamente, se liberan datos personales en un ambiente no confiable. Puede ocurrir en cualquier fase del tratamiento de datos y podría afectar los derechos patrimoniales o morales de los titulares, los tipos de vulneraciones que pueden ocurrir son:

a) Pérdida o destrucción no autorizada.
b) Robo, extravío o copia no autorizada.
c) Uso, acceso o tratamiento no autorizado.
d) Daño, alteración o modificación no autorizada.

La persona Responsable del Sistema de Datos Personales deberá informar, dentro de un plazo máximo de setenta y dos horas, al titular de los datos personales, a la Unidad de Transparencia, quien a su vez notificará al Órgano Garante, sin dilación alguna, en cuanto se confirme que ocurrió la vulneración y la persona Responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.

Asimismo, la persona Responsable realizará las acciones necesarias para la revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados tomen en su caso, las medidas correspondientes para la defensa de sus derechos. El Órgano Garante podrá verificar las medidas de mitigación, niveles de seguridad y documento de gestión para recomendar las medidas pertinentes para la protección de los datos del titular. El plazo a que se refiere el párrafo anterior comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

En caso de que ocurra una vulneración a la seguridad de los datos personales, que afecten de forma significativa los derechos personales y patrimoniales se deberá informar al titular, al menos lo siguiente:

a) La naturaleza del incidente.
b) Los datos personales comprometidos.
c) Los derechos del titular que pueda adoptar para proteger sus datos.
d) Las acciones correctivas realizadas de forma inmediata.
e) Los medios donde puede obtener más información al respecto.
f) La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
g) Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

La persona Responsable del SDP deberá notificar el informe directamente al titular de la información a través de los medios que establezca para tal fin. Para seleccionar y definir los medios de comunicación, la persona Responsable deberá considerar, según ello resulte aplicable, el perfil de las personas titulares, la forma en que mantiene contacto o comunicación con éstos, que sean gratuitos; de fácil acceso, con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el titular.

El registro de incidencias, que puede ser cualquier incumplimiento o anomalía (vulneración), es uno de los apartados que integran el Documento de Seguridad, mencionado en el Capítulo VII, y consiste en que la persona Responsable del SDP debe documentar esta incidencia mediante una bitácora, con el fin de que las personas encargadas de la seguridad den respuesta a los incidentes. También este registro, permite contar con más conocimientos, los cuales pueden ser utilizados para entrenar a los usuarios y cómo responder ante posibles incidentes, en pro de una mejora continua.

Se recomienda que la bitácora contenga por lo menos los siguientes elementos:

a) Tipo de vulneración.
b) Fecha y hora en que ocurrió la vulneración.
c) Motivos de la vulneración.
d) Acciones correctivas implementadas de forma inmediata y a largo plazo, derivadas de la incidencia.

CAPÍTULO X.
CUMPLIMIENTOS

De conformidad con los artículos 132, de la LGPDPPSO, en correlación con el 127, de la LPDPPSOCDMX, serán causas de sanción 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. 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;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la normativa aplicable;
V. No recabar el consentimiento del titular, lo que constituye que el tratamiento sea ilícito, o no contar con el aviso de privacidad, o bien tratar de manera dolosa o con engaños datos personales y las demás disposiciones que resulten aplicables en la materia;
VI. Incumplir el deber de confidencialidad;
VII. No establecer las medidas de seguridad;
VIII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;
IX. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la normativa aplicable;
X. Obstruir los actos de verificación de la autoridad;
XI. Crear bases de datos personales o sistemas de datos personales en contravención a lo dispuesto por el artículo 5 de la LPDPPSOCDMX;
XII. No acatar las resoluciones emitidas por el organismo garante; y
XIII. Omitir la entrega del informe anual y demás informes o bien, entregarlo de manera extemporánea.

Sin perjuicio de lo anterior, será obligación de todo el personal de cada una de las unidades administrativas de esta Secretaría, proteger y resguardar debidamente la información que contenga Datos Personales, para lo cual deberán tomar las medidas necesarias para evitar que la información o documentos que se encuentran bajo su custodia o de sus personas servidoras públicas o quienes tengan acceso o conocimiento con motivo de su empleo, cargo o comisión, hagan mal uso de ésta, la sustraigan, divulguen, alteren o destruyan, sin causa legítima, además de asegurar su custodia, conservación, integridad y disponibilidad.

TRANSITORIOS

Primero. Publíquense el presente Acuerdo por el que se crean las Políticas Internas de Protección de Datos Personales de la Secretaría de Salud Pública de la Ciudad de México, el cual cuenta con un anexo digital adjunto a este Acuerdo como parte integrante del mismo, en la Gaceta Oficial de la Ciudad de México,

Segundo. Entrarán en vigor al día siguiente de su publicación.

Tercero. Difúndanse en el Micrositio de Transparencia de Secretaría de Salud Pública de la Ciudad de México, así como de manera personalizada a los Titulares de las unidades administrativas y a sus Enlaces de Transparencia.

Ciudad de México, a 19 de noviembre de 2025
(Firma)
DRA. NADINE FLORA GASMAN ZYLBERMANN
SECRETARIA DE SALUD PÚBLICA DE LA CIUDAD DE MÉXICO