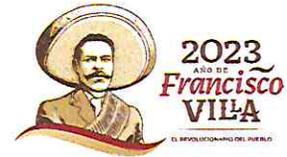




GOBIERNO DE LA
CIUDAD DE MÉXICO

SECRETARÍA DE SEGURIDAD CIUDADANA

DIRECCIÓN EJECUTIVA DE LA UNIDAD DE TRANSPARENCIA



UNIDAD DE TRANSPARENCIA



ÍNDICE

1. PRESENTACIÓN.

2. MARCO JURÍDICO – ADMINISTRATIVO.

3. OBJETIVO GENERAL DE LOS LINEAMIENTOS.

4. DEFINICIONES.

5. DE LAS ÁREAS Y ÓRGANO COMPETENTE.

- 5.1 DE LA UNIDAD DE TRANSPARENCIA;
- 5.2 DEL COMITÉ DE TRANSPARENCIA;
- 5.3 DE LAS ÁREAS;
- 5.4 DE LAS ÁREAS CON SISTEMAS DE DATOS PERSONALES;
- 5.5 DE LAS ÁREAS CONCENTRADORAS DE INFORMACIÓN;
- 5.6 DE LOS ENLACES.

6. DEL TRÁMITE DE LAS SOLICITUDES.

- 6.1 DE LA RECEPCIÓN Y REGISTRO DE LAS SOLICITUDES;
- 6.2 DE LA GESTIÓN DE SOLICITUDES;
- 6.3. DE LA COMPETENCIA;
- 6.4 DE LA PREVENCIÓN;
- 6.5 DEL PLAZO DE RESPUESTA Y AMPLIACIÓN DE PLAZO.

7. DEL CONTENIDO DE LAS RESPUESTAS.

- 7.1 DE LA FUNDAMENTACIÓN Y MOTIVACIÓN;
- 7.2 DE LAS SOLICITUDES QUE REQUIERAN LA REALIZACIÓN DE UN TRÁMITE;
- 7.3 DEL PROCESAMIENTO DE LA INFORMACIÓN.

8. DE LA CLASIFICACIÓN DE INFORMACIÓN Y DE LA INEXISTENCIA.

- 8.1 DE LAS MODALIDADES DE CLASIFICACIÓN DE INFORMACIÓN;
- 8.2 DEL PROCEDIMIENTO PARA LA CLASIFICACIÓN DE LA INFORMACIÓN Y VERSIONES PÚBLICAS;

Handwritten signatures in blue ink, including a large signature at the top right and several smaller ones below it.

Handwritten signatures in blue ink at the bottom right of the page.



- 8.3 DE LA AMPLIACIÓN DEL PLAZO DE RESERVA;
- 8.4 DE LOS ÍNDICES DE INFORMACIÓN PREVIAMENTE CLASIFICADA COMO RESERVADA;
- 8.5 DE LA INEXISTENCIA DE INFORMACIÓN Y DE DATOS PERSONALES;

9. DE LAS OBLIGACIONES DE TRANSPARENCIA.

- 9.1 DE LA TRANSPARENCIA PROACTIVA.

10. DE LA ATENCIÓN A LAS VERIFICACIONES Y DENUNCIAS.

- 10.1 DEL PROCEDIMIENTO DE VERIFICACIÓN A LAS OBLIGACIONES DE TRANSPARENCIA;
- 10.2 DEL PROCEDIMIENTO DE VERIFICACIÓN A LOS PRINCIPIOS Y DISPOSICIONES CONTENIDAS EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO Y DEMÁS ORDENAMIENTOS DERIVADOS DE ESTA;
- 10.3 DE LAS DENUNCIAS POR INCUMPLIMIENTO A LAS OBLIGACIONES DE TRANSPARENCIA;

11. DE LOS RECURSOS DE REVISIÓN.

- 11.1 EN MATERIA DE ACCESO A LA INFORMACIÓN;
- 11.2 DE LAS MANIFESTACIONES, PRUEBAS Y ALEGATOS;
- 11.3 DEL CUMPLIMIENTO DE LAS RESOLUCIONES;

12. DE LOS RECURSOS DE INCONFORMIDAD.

- 12.1 EN MATERIA DE ACCESO A LA INFORMACIÓN;
- 12.2 RESPECTO DEL EJERCICIO DE LOS DERECHOS ARCO;

13. DE LA CAPACITACIÓN Y DE LA CULTURA DE LA TRANSPARENCIA.

- 13.1 DE LA CAPACITACIÓN A LOS SERVIDORES PÚBLICOS;
- 13.2 DE LA PARTICIPACIÓN EN LA PROMOCIÓN DE LA CULTURA DE LA TRANSPARENCIA, EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y RENDICIÓN DE CUENTAS.

14. DE LAS SANCIONES Y RESPONSABILIDADES.

15. VALIDACIÓN DE LA ACTUALIZACIÓN DE LOS LINEAMIENTOS PARA LA OPERACIÓN DE LA UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO.

[Handwritten signatures and initials in blue ink, including a large 'T' and several illegible marks]



1. PRESENTACIÓN.

Derivado de la entrada en vigor de la Ley General de Transparencia, publicada el día 4 de mayo del 2015, reglamentaria del artículo 6º de nuestra Constitución Mexicana, así como la Ley de Transparencia, Acceso a Información Pública y Rendición de Cuentas de la Ciudad de México publicada el día 6 de mayo de 2016, se creó el Sistema Nacional de Transparencia cuyo objeto es fortalecer la rendición de cuentas del estado Mexicano, coordinando y evaluando las acciones relativas a la política pública transversal de transparencia, acceso a la información y la protección de datos personales, a través de la implementación de criterios y lineamientos que regulan el actuar de los organismos garantes así como de los sujetos obligados en esas materias, estableciéndose así mismo, nuevas obligaciones para los sujetos obligados.

Se crea además una Plataforma Nacional de Transparencia con la finalidad de sustituir en la Ciudad de México al sistema de solicitudes de información de la Ciudad de México denominado INFOMEX y a la Ventana Única de Transparencia (VUT), en la que se establecen cuatro sistemas denominados Sistema de Comunicación entre Organismos Garantes y Sujetos Obligados (SICOM), Sistema de Gestión de Medios de Impugnación (SIGEMI), Sistema de Portales de Obligaciones de Transparencia (SIPOT) y Sistema de Solicitudes de Acceso a la Información (SISAI), que permitirán a los sujetos obligados cumplir con los procedimientos obligaciones y disposiciones establecidas en la Ley General y la Ley local de Transparencia.

La Unidad de Transparencia antes Oficina de Información Pública, es la unidad administrativa que tutela la recepción y el trámite de las solicitudes de acceso a la información pública y de las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición al tratamiento de datos personales (derechos ARCO), realizando las gestiones internas con las diversas áreas del sujeto obligado, siendo además el vínculo entre las personas, los demás Sujetos Obligados y los Órganos garantes.

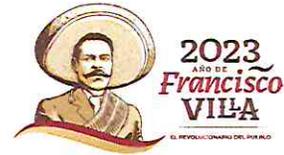
Con el propósito de eficientar la atención a las solicitudes de acceso a la información pública y las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición al tratamiento de datos personales (derechos ARCO), y servir como una herramienta a disposición de los servidores públicos de las distintas áreas de esta Secretaría de Seguridad Ciudadana de la Ciudad de México, para el cumplimiento de las obligaciones que en esas materias se establecen en la normatividad respectiva, en observancia a lo establecido en los artículos 44 fracciones I y IV y 45 fracción VI de la Ley General de Transparencia y Acceso a la Información Pública, así como a lo dispuesto por el los artículos 90 fracciones I y XIII y 93 fracción III de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y artículo 76 fracción V de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, se emitieron los presentes **LINEAMIENTOS PARA LA OPERACIÓN DE LA UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO.**

Handwritten signatures and initials in blue ink on the right margin of the document.



Por lo anterior y en atención al Decreto por el que se Reforman Adicionan y Derogan diversas Disposiciones del Reglamento Interior de la Secretaría de Seguridad Ciudadana, publicado en la Gaceta Oficial de la Ciudad de México el día 18 de octubre del 2021, y en el que se incorpora en el artículo 3, numeral 6 bis, a la Subsecretaría del Sistema Penitenciario como parte de las áreas que conforman la Secretaría de Seguridad Ciudadana de la Ciudad de México; a la actualización del Manual de Integración y Funcionamiento del Comité de Transparencia de esta Secretaría, publicado en la Gaceta Oficial de la Ciudad de México el día 9 de agosto de 2022 y en el que se contempla como integrante de ese Órgano Colegiado, a la Subsecretaría del Sistema Penitenciario, así como a las reformas a diversos numerales de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas aprobadas por los integrantes de la Comisión Jurídica, de Criterios y Resoluciones del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en su Tercera Sesión Ordinaria y Primera Sesión Extraordinaria, celebradas, respectivamente los días 22 de agosto y 05 de septiembre del año 2022 dos mil veintidós, resulta necesaria la actualización a los presente lineamientos, conforme a lo establecido en la fracción III del artículo 93 de la Ley de Transparencia Local.

[Handwritten signatures and initials in blue ink, including a large signature at the top right and several smaller ones below it.]



2. MARCO JURÍDICO-ADMINISTRATIVO.

- **CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.**
D.O.F. 17-05-2021. Vigente.
- **CONSTITUCIÓN POLÍTICA DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 02-09-2021. Vigente.
- **LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.**
D.O.F. 4- 05- 2015. Vigente.
- **LEY GENERAL DE PROTECCION DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS.**
DOF 26-01-2017. Vigente.
- **LEY GENERAL DE ARCHIVOS.**
D.O.F 15-06-2018. Vigente.
- **LEY ORGÁNICA DEL PODER EJECUTIVO Y DE LA ADMINISTRACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO.**
G.O.C.D.M.X. 13-12-2018 Vigente.
- **LEY DEL SISTEMA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO.**
G.O.C.D.M.X. 1-08-2019. Vigente.
- **LEY ORGÁNICA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 23-12-2019. Vigente.
- **LEY DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO.**
G.O.D.F. 6-05-2016. Vigente.
- **LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 10-04-2018. Vigente.
- **LEY DE ARCHIVOS DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 18-11-2020. Vigente.
- **LEY DE RESPONSABILIDADES ADMINISTRATIVAS DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 1-09-2017. Vigente.



- **LEY DE PROCEDIMIENTO ADMINISTRATIVO DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. EL 21-12-1995. Vigente.
- **LEY DE AUSTERIDAD, TRANSPARENCIA EN REMUNERACIONES, PRESTACIONES Y EJERCICIO DE RECURSOS DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 31-12-2018. Vigente.
- **CÓDIGO FISCAL DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 30-12-2021. Vigente.
- **CÓDIGO DE PROCEDIMIENTOS CIVILES PARA EL DISTRITO FEDERAL.**
G.O.CDMX. 18-07-2018. Vigente.
- **REGLAMENTO INTERIOR DEL PODER EJECUTIVO Y DE LA ADMINISTRACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 02-01-2019. Vigente.
- **REGLAMENTO INTERIOR DE LA SECRETARÍA DE SEGURIDAD CIUDADANA**
G.O.CDMX. 25-02-2020. Vigente.
- **MANUAL ADMINISTRATIVO DE LA SECRETARÍA DE SEGURIDAD CIUDADANA.**
G.O.CDMX. 27-02-2022. Vigente.
- **MANUAL DE INTEGRACIÓN Y FUNCIONAMIENTO DEL COMITÉ DE TRANSPARENCIA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO.**
G.O. CDMX. 09-09-2022. Vigente.
- **PROCEDIMIENTO PARA LA RECEPCIÓN, SUBSTANCIACIÓN, RESOLUCIÓN Y SEGUIMIENTO DE LOS RECURSOS DE REVISIÓN INTERPUESTOS EN MATERIA DE ACCESO A LA INFORMACIÓN PÚBLICA Y DE PROTECCIÓN DE DATOS PERSONALES EN LA CIUDAD DE MÉXICO.**
G.O. CDMX. 17-06-2016. Vigente.
- **LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 15-02-2022. Vigente.
- **LINEAMIENTOS PARA LA IMPLEMENTACIÓN Y OPERACIÓN DE LA PLATAFORMA NACIONAL DE TRANSPARENCIA.**
DOF: 04/05/2016. Vigente.



- **LINEAMIENTOS TÉCNICOS PARA PUBLICAR, HOMOLOGAR Y ESTANDARIZAR LA INFORMACIÓN DE LAS OBLIGACIONES ESTABLECIDAS EN EL TÍTULO QUINTO DE LA LEY DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO.**
G.O.CDMX. 23-09-2021. Vigente.
- **LINEAMIENTOS PARA DETERMINAR LOS CATÁLOGOS Y PUBLICACIÓN DE INFORMACIÓN DE INTERÉS PÚBLICO; Y PARA LA EMISIÓN Y EVALUACIÓN DE POLÍTICAS DE TRANSPARENCIA PROACTIVA.**
DOF 15-04-2016. Vigente.
- **LINEAMIENTOS QUE DEBERÁN OBSERVAR LOS SUJETOS OBLIGADOS PARA LA ATENCIÓN DE REQUERIMIENTOS OBSERVACIONES, RECOMENDACIONES Y CRITERIOS QUE EMITA EL SISTEMA NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES.**
DOF 4/05/2016. Vigente.
- **LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN, ASÍ COMO PARA LA ELABORACIÓN DE VERSIONES PÚBLICAS.**
DOF 29-07-2016. Vigente.
- **LINEAMIENTOS PARA LA GESTIÓN DE SOLICITUDES DE INFORMACIÓN PÚBLICA Y DE DATOS PERSONALES EN LA CIUDAD DE MÉXICO.**
G.O. CDMX. 17-06-2016. Vigente.
- **LINEAMIENTOS TÉCNICOS PARA LA INSTALACIÓN Y FUNCIONAMIENTO DE LOS COMITÉS DE TRANSPARENCIA DE LOS SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO.**
G.O. CDMX. 03-07-2020. Vigente.



3. OBJETIVO GENERAL DE LOS LINEAMIENTOS.

Establecer las políticas de actuación, criterios y directrices de operación, funcionamiento y organización que deberán observarse para el debido cumplimiento de la normatividad aplicable en materia de Transparencia, Protección de Datos Personales y Rendición de Cuentas en la Secretaría de Seguridad Ciudadana de la Ciudad de México.

(Handwritten signatures and marks in blue ink on the right side of the page)



4. DEFINICIONES.

Además de las establecidas en la normatividad aplicable en materia de transparencia y protección de datos personales, para efectos de los presentes lineamientos, se entenderá por:

Ajustes Razonables: A las modificaciones y adaptaciones necesarias y adecuadas que no impongan una carga desproporcionada o indebida, cuando se requieran en un caso particular, para garantizar a las personas con discapacidad el goce o ejercicio, en igualdad de condiciones, de los derechos humanos;

II. **Áreas:** Aquellas que estén previstas en la Ley Orgánica de la Secretaría de Seguridad Ciudadana de la Ciudad de México, su reglamento o su manual administrativo y que cuentan o puedan contar con información o ser responsables de sistemas de datos personales;

III. **Aviso de privacidad:** Documento a disposición del titular de los datos personales, generado por el responsable, de forma física, electrónica o en cualquier formato, previo a la recabación y tratamiento de sus datos, con el objeto de informarle sobre la finalidad del tratamiento, los datos recabados, así como la posibilidad de acceder, rectificar, oponerse o cancelar el tratamiento de los mismos;

IV. **Colaborador:** Aquellas personas que desempeña un empleo, cargo, comisión o que presta un servicio personal subordinado en la Secretaría de Seguridad Ciudadana de la Ciudad de México;

V. **Áreas concentradoras:** Aquellas que estén previstas en la Ley Orgánica de la Secretaría de Seguridad Ciudadana de la Ciudad de México, su reglamento o su manual administrativo y que de acuerdo a sus atribuciones o funciones cuentan con la mayor información en el llenado de los formatos establecidos por los órganos garantes para el cumplimiento a las obligaciones de transparencia.

VI. **Comité de Transparencia:** Al Órgano Colegiado de la Secretaría de Seguridad Ciudadana de la Ciudad de México cuya función es determinar la naturaleza de la Información.

VII. **Consejo Nacional:** Al Órgano Colegiado rector del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

VIII. **Consejo Local.** Al Órgano Colegiado rector del Sistema Local.

IX. **Consulta Directa:** A la prerrogativa que tiene toda persona de allegarse de información pública, sin intermediarios.

X. **Datos abiertos:** A los datos digitales de carácter público que son accesibles en línea que pueden ser usados, reutilizados y redistribuidos por cualquier interesado y que tienen las siguientes



características:

- a) **Accesibles:** Los datos están disponibles para la gama más amplia de usuarios, para cualquier propósito;
- b) **De libre uso:** Citan la fuente de origen como único requerimiento para ser utilizados libremente;
- c) **En formatos abiertos:** Los datos estarán disponibles con el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no suponen una dificultad de acceso y que su aplicación y reproducción no estén condicionadas a contraprestación alguna;
- d) **Gratuitos:** Se obtienen sin entregar a cambio contraprestación alguna;
- e) **Integrales:** Contienen el tema que describen a detalle y con los metadatos necesarios;
- f) **Legibles por máquinas:** Deberán estar estructurados, total o parcialmente, para ser procesados e interpretados por equipos electrónicos de manera automática;
- g) **No discriminatorios:** Los datos están disponibles para cualquier persona, sin necesidad de registro;
- h) **Oportunos:** Son actualizados, periódicamente, conforme se generen;
- i) **Permanentes:** Se conservan en el tiempo, para lo cual, las versiones históricas relevantes para uso público se mantendrán disponibles con identificadores adecuados al efecto;
- j) **Primarios:** Proviene de la fuente de origen con el máximo nivel de desagregación posible;

- XI. **Datos Personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona.
- XII. **Datos Personales Sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, 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 aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;
- XIII. **Derechos ARCO:** Los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales;

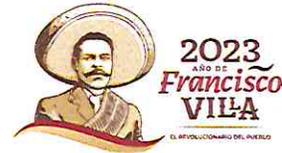




- XIV. **Derecho de Acceso a la Información Pública:** A la prerrogativa que tiene toda persona para acceder a la información generada, administrada o en poder de esta Secretaría, en los términos de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;
- XV. **Documento:** A los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones, competencias y decisiones de los sujetos obligados, sus personas servidoras públicas e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;
- XVI. **Documento Electrónico:** A la Información que puede constituir un documento, archivada o almacenada en un soporte electrónico, en un formato determinado y susceptible de identificación y tratamiento.
- XVII. **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;
- XVIII. **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;
- XIX. **Expediente:** A la unidad documental constituida por uno o varios documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados;
- XX. **Expediente Electrónico:** Al conjunto de documentos electrónicos cuyo contenido y estructura permiten identificarlos como documentos de archivo que aseguran la validez, autenticidad, confidencialidad, integridad y disponibilidad de la información que contienen.
- XXI. **Estrados:** Medio por el cual se le notifica a los peticionarios de Información Pública o Datos Personales, el resultado de su solicitud, cuando estos no proporcionan medio alguno para que les sea entregada la misma.
- XXII. **Formatos Abiertos:** Al conjunto de características técnicas y de presentación de la información que corresponden a la estructura lógica usada para almacenar datos de forma integral y facilitan su procesamiento digital, cuyas especificaciones están disponibles públicamente y que permiten el acceso sin restricción de uso por parte de los usuarios;
- XXIII. **Formatos Accesibles:** Al acceso a la información de cualquier manera o forma alternativa, en forma tan viable o cómoda para cualquier persona, eliminando las barreras o dificultades para las personas con discapacidad para acceder a cualquier texto impreso y/o cualquier otro formato convencional en el que la información pueda encontrarse.



- XXIV. Igualdad Sustantiva:** Al mismo trato y oportunidades para el reconocimiento, goce o ejercicio del Derecho al Acceso a la Información Pública.
- XXV. Indicador de Resultados:** A la información que permita evaluar el cumplimiento de las metas y objetivos institucionales, indicando los beneficios obtenidos, de acuerdo a los resultados de la gestión.
- XXVI. Información Confidencial:** A la información en poder de esta Secretaría, protegida por el derecho fundamental a la Protección de los Datos Personales y la privacidad;
- XXVII. Información Clasificada:** A la información en posesión de esta Secretaría, bajo las figuras de reservada o confidencial;
- XXVIII. Información de interés público:** A la información que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que lleva a cabo esta Secretaría;
- XXIX. Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales;
- XXX. Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;
- XXXI. 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 consideran 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;
- XXXII. Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se consideran las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos



personales;

XXXIII. Obligaciones de Transparencia: Aquella contemplada respectivamente en el Título Quinto, Capítulo II De las obligaciones de transparencia comunes de la Ley General de Transparencia y de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y que deberán publicarse en la Plataforma Nacional de Transparencia y Portal de Transparencia de esta Secretaría;

XXXIV. Información Reservada: A la información pública que se encuentra temporalmente sujeta a alguna de las excepciones previstas en Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;

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

XXXVI. INAI: Al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XXXVII. Ley: A la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;

XXXVIII. LG: A la Ley General de Transparencia y Acceso a la Información Pública;

XXXIX. LPDPPSOCDMX: A la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

XL. Lineamientos y Criterios: A los instrumentos normativos emitidos por el INAI, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el Instituto y el Sistema Local de Transparencia, Acceso a la Información, Protección de Datos Personales, Apertura Gubernamental y Rendición de Cuentas de la Ciudad de México;

XLI. Lineamientos: Al Instrumento por el cual se regula la gestión interna de los servidores públicos de esta Secretaría, para dar cumplimiento a las obligaciones que en materia de transparencia, protección de datos personales y rendición de cuentas establece la normatividad correspondiente;

XLII. Personas Servidoras Públicas: A los mencionados en el párrafo primero del Artículo 108 de la Constitución Política de los Estados Unidos Mexicanos y sus correlativos establecidos en la normatividad aplicable en la Ciudad de México;

XLIII. Pleno: Al Órgano Colegiado directivo del Instituto;

XLIV. Prueba de Daño: A la Carga de los titulares de las áreas o Unidades Administrativas competentes de demostrar que la divulgación de información solicitada lesiona el interés jurídicamente protegido por la Ley, y que el daño que pueda producirse con la publicidad de la información es mayor que el interés de conocerla;

XLV. Prueba de Interés Público: A la facultad del Instituto de fundar y motivar con base en elementos de

CIUDAD INNOVADORA
Y DE DERECHOS



idoneidad, necesidad y proporcionalidad, que la publicación de la información de acceso restringido no lesiona el interés jurídicamente protegido por la Ley;

XLVI. Plataforma Nacional: a la Plataforma Nacional de Transparencia, como el medio electrónico oficial a nivel Federal y Estatal para gestionar las solicitudes de acceso a la información, protección de datos personales, obligaciones de transparencia, medios de impugnación y la comunicación entre organismos garantes y esta Secretaría, integrada por cuatro sistemas denominados: Sistema de Comunicación entre Organismos Garantes y Sujetos Obligados (SICOM), Sistema de Gestión de Medios de Impugnación (SIGEMI), Sistema de Portales de Obligaciones de Transparencia (SIPOT) y Sistema de Solicitudes de Acceso a la Información (SISAI), a través de la cual se ejercerán los derechos de acceso a la información y Protección de Datos Personales en posesión de esta Secretaría en cumplimiento a los procedimientos obligaciones y disposiciones establecidas en la Ley General y la Ley Local de Transparencia.

XLVII. Rendición de Cuentas: Vista desde la perspectiva de la transparencia y el acceso a la información, consiste en la potestad del individuo para exigir al poder público informe y ponga a disposición en medios adecuados, las acciones y decisiones emprendidas derivadas del desarrollo de su actividad, así como los indicadores que permitan el conocimiento y la forma en que las llevó a cabo, incluyendo los resultados obtenidos; así como la obligación de dicho poder público de cumplir con las obligaciones que se le establecen en la legislación de la materia, y garantizar mediante la implementación de los medios que sean necesarios y dentro del marco de la Ley, el disfrute del Derecho de Acceso a la Información Pública consagrado en el artículo sexto de la Constitución General de la República;

XLVIII. Recurso de Revisión: Medio de impugnación que tienen los peticionarios, cuando consideran no satisfecho su derecho de acceso a la información, o que se consideren agraviados por la resolución definitiva que le recaiga a su solicitud de acceso, rectificación, cancelación o ante la omisión de respuesta.

XLIX. Reglamento: Al Reglamento de la LTAIPRC.

L. Recurso de inconformidad: Medio de impugnación que tienen los peticionarios, en contra de las resoluciones emitidas por el Instituto que confirmó o modificó la clasificación de la información o confirmó la inexistencia o negativa de información solicitada.

LI. Responsable de Seguridad: Persona a la que el Responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables;

LII. Sistema Local: Al Sistema Local de Transparencia, Acceso a la Información, Protección de Datos Personales, Apertura Gubernamental y Rendición de Cuentas de la Ciudad de México;

LIII. Sistema Nacional: Al Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

LIV. Sistema Electrónico: A la Plataforma Nacional de Transparencia, o cualquier otro medio

Handwritten blue ink marks and signatures on the right margin, including a large '9' at the top, a vertical line, and several scribbles and initials.



electrónico habilitado por los Órganos Garantes, para gestionar las solicitudes de acceso a la información, protección de datos personales, obligaciones de transparencia, medios de impugnación y la comunicación entre estos y la Secretaría;

- LV. **Sistema de Datos Personales:** Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de esta Secretaría, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso;
- LVI. **Secretaría:** A la Secretaría de Seguridad Ciudadana de la Ciudad de México;
- LVII. **Titular:** La persona física a quien corresponden los datos personales;
- LVIII. **Transparencia Proactiva:** El conjunto de actividades que promueven la identificación, generación, publicación y difusión de información adicional a la establecida con carácter obligatorio por la Ley General, que permite la generación de conocimiento público útil con un objeto claro enfocado en las necesidades de sectores de la sociedad determinados o determinables.
- LIX. **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales;
- LX. **Usuario:** Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.
- LXI. **UT:** A la Unidad de Transparencia de la Secretaría de Seguridad Ciudadana de la Ciudad de México, receptora de las solicitudes del derecho de acceso a la información pública y derechos ARCO, y a cuya tutela estará el trámite de las mismas; y
- LXII. **Versión Pública:** A la información a la que se da acceso eliminando u omitiendo partes o secciones clasificadas.

[Handwritten signatures and initials in blue ink, including a large 'J' and 'P' and various initials]





5. DE LAS ÁREAS Y ÓRGANO COMPETENTE.

5.1 De la Unidad de Transparencia.

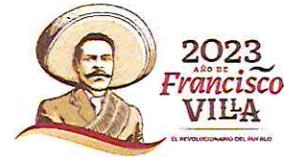
La Dirección Ejecutiva de la Unidad de Transparencia se encuentra a cargo de la UT y es el área encargada de recibir, capturar, ordenar, analizar, procesar y dar trámite a las solicitudes de acceso a la información pública y del ejercicio de los derechos ARCO que ingresen a esta Secretaría, dándoles seguimiento hasta la entrega de la respuesta correspondiente, así como atender los recursos de revisión y de inconformidad que se deriven de las mismas a través de su personal. Asimismo, se encarga de verificar y coordinar la publicación de las obligaciones de transparencia.

Además, su titular funge como enlace en materia de datos personales ante el Instituto y es Secretaria (o) Técnica (o) del Comité de Transparencia, teniendo las atribuciones que le confieren la Ley de Transparencia y Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, su Reglamento, la LPDPPSOCDMX y sus lineamientos, el Manual Administrativo de esta Secretaría y los presentes lineamientos de Operación.

Tanto el responsable de la UT como el personal directamente relacionado con la atención a solicitudes deberán tener conocimiento de la normatividad en materia de transparencia, acceso a la información pública y protección de datos personales, de la estructura orgánica y atribuciones de las áreas que conforman esta Secretaría y la Administración Pública de la Ciudad de México.

Son atribuciones de la Unidad de Transparencia conforme a la Ley:

- I. Capturar, ordenar, analizar y procesar las solicitudes de información presentadas ante el sujeto obligado;
- II. Recabar, publicar y actualizar las obligaciones de transparencia a las que refiere la Ley;
- III. Proponer al Comité de Transparencia del sujeto obligado, los procedimientos internos que contribuyan a la mayor eficiencia en la atención de las solicitudes de acceso a la información;
- IV. Recibir y tramitar las solicitudes de información, así como darles seguimiento hasta la entrega de la misma, haciendo entre tanto el correspondiente resguardo;
- V. Llevar el registro de las solicitudes de acceso a la información, y actualizarlo trimestralmente, así como sus trámites, costos y resultados, haciéndolo del conocimiento del Comité de Transparencia correspondiente;
- VI. Asesorar y orientar de manera sencilla, comprensible y accesible a los solicitantes sobre:
 - a) La elaboración de solicitudes de información;
 - b) Trámites y procedimientos que deben realizarse para solicitar información; y



c) Las instancias a las que puede acudir a solicitar orientación, consultas o interponer quejas sobre la prestación del servicio.

VII. Efectuar las notificaciones correspondientes a los solicitantes;

VIII. Habilitar a las personas servidoras públicas de los sujetos obligados que sean necesarios, para recibir y dar trámite a las solicitudes de acceso a la información;

IX. Formular el programa anual de capacitación en materia de Acceso a la Información y apertura gubernamental, que deberá de ser instrumentado por la propia unidad;

X. Apoyar al Comité de Transparencia en el desempeño de sus funciones;

XI. Establecer los procedimientos para asegurarse que, en el caso de información confidencial, ésta se entregue sólo a su titular o representante;

XII. Operar los sistemas digitales que para efecto garanticen el Derecho a Acceso a Información;

XIII. Fomentar la Cultura de la Transparencia; y

XIV. Las demás previstas en esta Ley, y demás disposiciones aplicables de la materia.

Son atribuciones de la Unidad de Transparencia conforme a la LPDPPSOCDMX:

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

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

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

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

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

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

VII. Asesorar a las áreas del sujeto obligado en materia de protección de datos personales;

VIII. Registrar ante el Instituto los sistemas de datos personales, así como su modificación y supresión;
y

Handwritten blue ink marks and signatures on the right margin, including a large 'T' and various scribbles.



IX. Hacer las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales en posesión del responsable.

La **Subdirección de Atención a Solicitudes de Información** tiene las siguientes funciones:

1. Coordinar la recepción, registro y atención de las solicitudes de información pública y datos personales, ingresadas a la Secretaría a través de los sistemas electrónicos habilitados por los Órganos Garantes, correo electrónico, por escrito y de manera presencial;
2. Supervisar la asignación de las solicitudes de información pública y de datos personales a las Unidades Administrativas competentes, para su atención;
3. Verificar el registro sobre los vencimientos de las solicitudes de información pública y de datos personales;
4. Coordinar la integración de las respuestas emitidas por las Unidades Administrativas a las solicitudes de información pública y de datos personales;
5. Asesorar a las unidades administrativas que lo requieran, en la atención de las solicitudes de información pública y datos personales;
6. Revisar las respuestas de las áreas a las solicitudes, así como emitir las observaciones que se consideren pertinentes;
7. Supervisar la elaboración de los acuerdos de caducidad de trámite de las solicitudes de información pública;
8. Administrar los Estrados de la Dirección Ejecutiva de la Unidad de Transparencia;
9. Coordinar la elaboración de los informes requeridos en su ámbito de competencia;
10. Coordinar el registro de los recursos de revisión y recursos de inconformidad, interpuestos en contra de esta Secretaría, con el fin de llevar un control adecuado para su atención oportuna;
11. Notificar a las unidades administrativas responsables respecto de la interposición de los recursos de revisión y recursos de inconformidad y requerir las manifestaciones y alegatos correspondientes;



12. Supervisar la elaboración de las respuestas complementarias que requieran las Unidades Administrativas, durante la substanciación del recurso de revisión;
13. Verificar el registro sobre los términos establecidos para la substanciación de los recursos de revisión y recursos de inconformidad y, en su caso, coordinar la elaboración de los oficios de recordatorio a las unidades administrativas;
14. Coordinar la integración de la información rendida por las Unidades Administrativas y elaborar las manifestaciones, diligencias para mejor proveer, alegatos y cumplimientos en la tramitación de los recursos de revisión y recursos de inconformidad y rendirlos en tiempo y forma;
15. Asesorar a las unidades administrativas que lo requieran en la atención de los recursos de revisión;

La **Subdirección de Transparencia** tiene las siguientes funciones:

1. Coordinar con las áreas y áreas concentradoras de información, la recabación, publicación y actualización de las obligaciones de transparencia, conforme a la normatividad aplicable;
2. Coordinar la gestión ante el Órgano Garante local, de los nombres y claves de usuario para las áreas que operan el Sistema de Portal de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia;
3. Coordinar con las áreas la creación, modificación, supresión y registro de los sistemas de datos personales ante el Órgano Garante así como el manejo, mantenimiento, seguridad y protección de los mismos;
4. Coordinar las reuniones de la red de enlaces de transparencia y protección de datos personales de la Secretaría;
5. Coordinar las acciones de capacitación y difusión en materia de transparencia y protección de datos personales;
6. Proponer a la Dirección Ejecutiva de la Unidad de Transparencia, el proyecto del programa anual de capacitación en materia de acceso a la información y apertura gubernamental en coordinación con el órgano garante local, para su aprobación por el Comité de Transparencia;
7. Apoyar a la Dirección Ejecutiva de la Unidad de Transparencia en las funciones de la Secretaría Técnica del Comité de Transparencia;



8. Coordinar la recepción y registro de las solicitudes de clasificación de información, supervisando que las mismas se encuentren fundadas y motivadas para ser sometidas a consideración del Comité de Transparencia;
9. Coordinar la elaboración y presentar a firma de la Dirección Ejecutiva de la Unidad de Transparencia, las convocatorias, proyectos de acuerdos, actas de Comité y demás en el área de su competencia;
10. Coordinar la recepción de las recomendaciones, observaciones, requerimientos y solicitudes de los órganos garantes en materia de datos personales, obligaciones de transparencia, capacitación y difusión de la cultura de la transparencia;
11. Supervisar las recomendaciones, observaciones, requerimientos y solicitudes de los órganos garantes para proponer a la Dirección Ejecutiva de la Unidad de Transparencia las áreas que considera competentes de atenderlas;
12. Coordinar la elaboración de los oficios de turno a las áreas competentes para atender las recomendaciones, observaciones, requerimientos y demás solicitudes de los órganos garantes para firma de la Dirección Ejecutiva de la Unidad de Transparencia;
13. Coordinar la atención seguimiento y cumplimiento de las denuncias notificadas por incumplimiento a las obligaciones de transparencia, con el área competente para su atención;
14. Brindar asesoría a las áreas en el ámbito de su competencia;
15. Supervisar los informes y reportes en el área de su competencia.

5.2 Del Comité de Transparencia.

Órgano Colegiado constituido y debidamente registrado ante el Instituto, cuyas atribuciones y funciones están definidas en el artículo 90 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, artículo 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y el Manual de Integración y Funcionamiento del Comité de Transparencia de esta Secretaría y tiene por objeto regular las acciones y procedimientos para asegurar la mayor eficiencia en la gestión de las solicitudes en materia de acceso a la información y las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición; confirmar, modificar o revocar la clasificación de información o declaración de inexistencia o incompetencia que realicen los titulares de las áreas, y establecer políticas para facilitar la obtención de información y el ejercicio del derecho a la información pública, así como promover la capacitación de los Servidores Públicos.



5.3 De las Áreas.

Son áreas principales de la Secretaría para el ejercicio de sus funciones en materia de transparencia y protección de datos, previstas en su Reglamento Interior las siguientes:

- Subsecretaría de Operación Policial
- Subsecretaría de Control de Tránsito
- Subsecretaría de Participación Ciudadana y Prevención del Delito
- Subsecretaría de Desarrollo Institucional
- Subsecretaría de Inteligencia e Investigación Policial
- Subsecretaría del Sistema Penitenciario
- Oficialía Mayor
- Dirección General de Asuntos internos
- Dirección General de Asuntos Jurídicos
- Dirección Ejecutiva de Comunicación Social
- Dirección de la Unidad de Contacto del Secretario

Los titulares de estas áreas y los titulares de las áreas adscritas a las antes referidas y sus enlaces designados en Transparencia, Protección de Datos Personales y (SIPOT), deberán coordinarse con la UT y el Comité de Transparencia en las funciones que tienen encomendadas en materia de transparencia, acceso a la información pública, protección de datos personales, archivo, capacitación, participación en eventos que fomenten la cultura de la transparencia, el derecho de acceso a la información pública y rendición de cuentas, así como en el cumplimiento de las demás obligaciones establecidas en la normatividad aplicable a las materias señaladas.

La relación de las áreas mencionadas es enunciativa más no limitativa en atención a las modificaciones en la estructura orgánica de esta Secretaría, para lo cual las áreas de nueva creación tendrán las mismas obligaciones establecidas en los presentes lineamientos, así como las que se desprendan de la normatividad aplicable.

5.4 De las Áreas con Sistemas de Datos Personales.

Será obligación de los titulares de las áreas responsables que traten datos personales, observar los principios de calidad, confidencialidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad, transparencia y temporalidad, establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico, contempladas en la normatividad aplicable para la protección de 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, para lo cual, deberán implementar acciones, controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, conozcan sus funciones, responsabilidades, las consecuencias de su incumplimiento, así como la obligación de rendir cuentas respecto del mismo, debiendo además de establecer



instrumentos en los que se les haga del conocimiento la obligación de guardar confidencialidad de los datos personales que traten, aun cuando haya finalizado su relación laboral con el responsable.

Deberán contar con un sistema de gestión denominado documento de seguridad, el cual se elaborará por el responsable conforme a la "GUÍA PARA LA ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD" y a los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, mismo que contendrá al menos, lo siguiente:

- I. El inventario de datos personales en los sistemas de datos;
- II. Las funciones y obligaciones de las personas que intervengan en el tratamiento datos personales, usuarios y encargados, en el caso de que los hubiera;
- III. Registro de incidencias;
- IV. Identificación y autenticación;
- V. Control de acceso; gestión de soportes y copias de respaldo y recuperación;
- VI. El análisis de riesgos;
- VII. El análisis de brecha;
- VIII. Responsable de seguridad;
- IX. Registro de acceso y telecomunicaciones;
- X. Los mecanismos de monitoreo y revisión de las medidas de seguridad;
- XI. El plan de trabajo; y
- XII. El programa general de capacitación.

El documento de Seguridad deberá de estar bajo el resguardo exclusivo del responsable del sistema de datos personales; únicamente se harán del conocimiento al responsable de seguridad, a los usuarios, y en su caso a los encargados, las medidas de seguridad, técnicas, físicas y administrativas que deberán de seguir en el tratamiento para la protección de los datos personales.

Será obligación del Responsable del sistema de datos personales, contemplar en su acta de entrega-recepción su Documento de Seguridad.

Ciudad INNOVADORA Y DE DERECHOS
(Handwritten signatures and initials)



Así mismo, cuando se trate de la creación de nuevas áreas en la estructura orgánica de esta Secretaría, con atribuciones para tratar datos personales de un sistema de datos personales existente, el Responsable del sistema de datos personales que se encuentre en el último acuerdo publicado en la Gaceta Oficial de la Ciudad de México, deberá coordinarse con el nuevo Responsable de dicho sistema para elaborar el acuerdo de modificación y remitirlo a la Dirección Ejecutiva de la Unidad de Transparencia por oficio.

Además, el Responsable del sistema de datos personales deberá transferir el documento de seguridad digitalizado e impreso y la totalidad de los expedientes físicos y automatizados generados durante su gestión, así como las actas de destrucción de expedientes conforme a la Ley de Archivos de la Ciudad de México, por oficio con una relación de la totalidad de archivos que se entregan.

El documento de Seguridad deberá actualizarse 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 ocurrida;
- IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad; y
- V. Por recomendación del Instituto.

Será obligación del Responsable del sistema de datos personales sin perjuicio de las establecidas en la (LPDPPSO) realizar las siguientes acciones:

- ✓ Elaborar oficio en el que se designe o ratifique al responsable de seguridad de su Sistema de Datos Personales;
- ✓ Elaborar oficio de autorización de las personas servidoras públicas que fungirán como USUARIOS de su sistema de datos personales para dar tratamiento y/o acceso a los datos personales;
- ✓ Acreditar la implementación de las medidas de seguridad con las que cuenta su Sistema de Datos Personales, las cuales deberán de estar documentadas en su documento de seguridad.



- ✓ Elaborar oficio dirigido a las personas servidoras públicas que fungen como USUARIOS de su sistema de datos personales, en el que se les haga del conocimiento sus funciones y obligaciones que tienen en el tratamiento de datos personales, las medidas de seguridad que deberán seguir en la protección de datos personales, así como las consecuencias de su incumplimiento, establecidas en el artículo 127 de la (LPDPPSO).
- ✓ Acreditar la capacitación de las personas servidoras públicas que tratan datos personales (RESPONSABLE) (RESPONSABLE DE SEGURIDAD) y (USUARIOS) en su sistema de datos personales en el curso Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y demás cursos que sean necesarios para el cumplimiento de la normatividad de la materia, y a los cuales podrán acceder de manera permanente e inscribirse en la liga siguiente:

<https://cava.infocdmx.org.mx/>

EN EL CASO DE LOS SISTEMAS DE DATOS PERSONALES QUE CUENTEN CON UN ENCARGADO, entendiéndose a este como:

“La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable”

(Fracción XV del artículo 3 de la LPDPPSO).

Será obligación del responsable del sistema, verificar o en su caso actualizar con el área jurídica (competente) de esta Secretaría que la relación jurídica con el ENCARGADO, se encuentre formalizada mediante un contrato o instrumento jurídico en el que se prevean como mínimo las cláusulas generales relacionadas con los servicios que presente el encargado señaladas en artículo 56 de la (LPDPPSO), las cuales de manera enunciativa más no limitativa serán las siguientes:

- I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
- II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables establecidos en la presente Ley y la naturaleza de los datos;
- IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
- V. Guardar confidencialidad respecto de los datos personales tratados; y
- VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.



[Handwritten signature]

En el caso de que el Responsable contrate o se adhiera a servicios, aplicaciones e infraestructura de cómputo en la nube, y otros servicios que impliquen el tratamiento de datos personales, el proveedor externo estará obligado a garantizar la protección de datos personales con los principios y deberes establecidos en la normatividad correspondiente y demás disposiciones que resulten aplicables en la materia, además deberá de delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos, las cuales el proveedor deberá:

I. cumplir con al menos los siguiente:

- a) Aplique políticas de protección de datos personales con base en los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;
- b) Transparente y limite las subcontrataciones que involucren el tratamiento de datos personales;
- c) Se abstenga 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) Guarde 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 protección de datos personales, privacidad o condiciones del servicio que presta;
- b) Permita al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
- c) Establezca y mantenga medidas de seguridad adecuadas y verificables para la protección de los datos personales sobre los que se preste el servicio;
- d) Garantice la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, e
- e) Impida el acceso a los datos personales a personas ajenas, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

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

En caso de que ocurra una vulneración a la seguridad de un Sistema de Datos Personales, se deberán analizar las causas por las cuales se presentó e implementar en el plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, a efecto de evitar que la vulneración se repita.





[Handwritten signature]

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, al menos, las siguientes:

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

[Handwritten signature]

Se 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.

[Handwritten signature]

Asimismo, se deberá informar sin dilación alguna al titular de los datos personales, y al Instituto, en cuanto se confirme que ocurrió la vulneración. El responsable realizará las acciones necesarias para la revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados tomen las medidas correspondientes para la defensa de sus derechos. El Instituto 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.

[Handwritten signature]

Deberán informar al titular de los datos personales al menos lo siguiente:

- I. La naturaleza del incidente;
- II. Los datos personales comprometidos;
- III. Los derechos del titular que pueda adoptar para proteger sus datos;
- IV. Las acciones correctivas realizadas de forma inmediata; y
- V. Los medios donde puede obtener más información al respecto.

[Handwritten signature]

Lo anterior sin demérito de que el Instituto pueda realizar una inspección o verificación sobre las medidas adoptadas para mitigar el impacto en los datos personales, así como emitir las recomendaciones que se solventarán en el tiempo establecido por el Instituto.

Para la creación, modificación o supresión de los Sistemas de Datos Personales, el Titular del área deberá remitir a la UT, su "proyecto de acuerdo", conforme al formato establecido por el Instituto, contenido en los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, para que una vez analizado, se realicen las gestiones correspondientes ante la Dirección General de Asuntos Jurídicos para su publicación.

[Handwritten signature]

[Handwritten signature]



Será obligación del Titular del área en su calidad de responsable del sistema (s), realizar su registro de creación, modificación o supresión, en el Registro Electrónico de Sistemas de Datos Personales (RESDP) habilitado por el Instituto, para lo cual se deberá acudir a la UT, a más tardar el día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México o cuando existan modificaciones que no requieran su publicación como: (Datos del Responsable), (Reformas a la Normatividad) o (nombre de Usuarios), con los datos a modificar en versión editable.

Para el registro correspondiente, se deberá contemplar como mínimo lo siguiente:

- I. Nombre y cargo del titular del sujeto obligado como responsable del tratamiento y los usuarios;
- II. Finalidad o finalidades del tratamiento;
- III. Naturaleza de los datos personales contenidos en cada sistema;
- IV. Formas de recabación, pertinencia, proporcionalidad y calidad de los datos;
- V. Las posibles transferencias;
- VI. Modo de interrelacionar la información registrada;
- VII. Ciclo de vida de los datos personales y tiempos de conservación (conforme a las disposiciones legales que en materia de archivos resulten aplicables, así como al Catálogo de Disposición Documental de esta Secretaría); y
- VIII. Medidas de seguridad.

Inclusión en el Catálogo de Disposición Documental

Determinar el ciclo de vida de los datos personales tratados, considerando los aspectos administrativos, contables, fiscales, jurídicos e históricos y realizar las gestiones necesarias ante el encargado de la Unidad Coordinadora de Archivos, para su inclusión en el Catálogo de Disposición Documental de esta Secretaría.

Aviso de Privacidad

Elaborar el aviso de privacidad integral y simplificado y su actualización, cuando existan cambios, conforme a los formatos contenidos en los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y remitir el mismo por oficio a la Dirección Ejecutiva de la Unidad de Transparencia, debiendo además acompañar los formatos mediante los cuales recaba datos personales con el aviso de privacidad inserto en los mismos.

Responsable de Seguridad

El Responsable del sistema de datos personales deberá remitir el oficio de designación de la persona servidora pública que fungirá como Responsable de Seguridad del sistema de datos personales con los datos siguientes:



Nombre completo del funcionario designado;

b) Cargo;

c) Área a la cual está adscrito;

d) Correo electrónico oficial;

e) Números de teléfono oficiales en los cuales pueda ser localizado fácilmente,

f) Domicilio oficial;

g) Así como la notificación de sus obligaciones como Responsable de Seguridad contenidas en los presentes lineamientos.

Funciones y Obligaciones del Responsable de Seguridad

• Obligaciones: además de las señaladas de manera genérica a los usuarios, deberá:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, el ciclo de vida de los Datos Personales (obtención, uso y supresión);

II. Definir las funciones y obligaciones del personal involucrado, elaborar el inventario de Datos Personales;

III. Realizar el análisis de riesgo considerando las amenazas y vulnerabilidades existentes;

IV. Solicitar los recursos involucrados en su tratamiento para la compra de hardware, software, contratación de personal del responsable;

V. Realizar el análisis de brecha;

VI. Elaborar un plan de trabajo e implementar las medidas de seguridad faltantes, las políticas de gestión y tratamiento;

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, las amenazas y vulneraciones;

VIII. Diseñar y aplicar capacitaciones del personal bajo su mando, dependiendo de sus roles y responsabilidades;

5.5 De las Áreas Concentradoras de Información.

Para el cumplimiento de las obligaciones de transparencia establecidas en la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, algunas de las áreas

Handwritten signatures and initials in blue ink, including 'F', 'OT', 'K', 'E', 'M', and 'R'.



generadoras o administradoras de la información de acuerdo a sus atribuciones y funciones, concentran la mayor información en el llenado de los formatos homologados contenidos en el Sistema de Portales de Obligaciones de Transparencia (SIPOT), en base a los lineamientos técnicos para publicar, homologar y estandarizar la información de las Obligaciones de Transparencia establecidas en el título quinto de la Ley de Transparencia, acceso a la información pública y rendición de cuentas de la Ciudad de México, por lo que estas áreas concentradoras, deberán coordinarse con las demás áreas no concentradoras, para el acopio de la información y llenado de los formatos homologados, realizando la carga de estos en la Plataforma Nacional de Transparencia una vez que la UT, haya supervisado que los formatos den cumplimiento a los criterios para su publicación establecidos en los lineamientos referidos.

Las áreas concentradoras de información de esta Secretaría de acuerdo a sus atribuciones y funciones son las siguientes:

- Subsecretaría de Inteligencia e Investigación Policial;
- Dirección General de Administración de Personal;
- Dirección General de Desarrollo Organizacional y Administrativo;
- Dirección General de Asuntos Internos;
- Dirección General de los Órganos Colegiados de Honor y Justicia.

La relación de las áreas mencionadas es enunciativa más no limitativa en atención a la creación de nuevas obligaciones en materia de transparencia o modificaciones a la estructura orgánica.

5.6 De los Enlaces.

Los titulares de las áreas de la Secretaría, deberán designar mediante oficio dirigido al Titular de la UT, a la persona servidora pública que fungirá como Enlace de transparencia, de la Plataforma Nacional de Transparencia, SIPOT y enlace de protección de datos personales, funciones que podrán recaer o no en uno mismo, debiendo considerar que él servidor público designado deberá tener cargo de estructura.

En caso de ausencia temporal del Enlace designado o cambio del mismo, el titular del área designará en el acto a otra persona servidora pública que realizará las funciones de Enlace para lo cual deberá informar de manera inmediata a la UT por oficio.

En ambos casos el oficio de designación de los enlaces que el titular del área envíe a la UT, deberá contener, como mínimo lo siguiente:

- a) Nombre completo del funcionario designado;
- b) Cargo;
- c) Área a la cual está adscrito;
- d) Correo electrónico oficial;



f

h

T

q

m

g

h

- e) Números de teléfono oficiales en los cuales pueda ser localizado fácilmente,
- f) Domicilio oficial;
- g) **Así como la notificación de sus obligaciones como enlace contenidas en los presentes lineamientos.**

Los titulares de las áreas deberán hacer del conocimiento al Enlace designado de manera oficial, todas y cada una de las obligaciones que tiene encomendadas en el ejercicio de su función, destacando de manera enunciativa y no limitativa, las siguientes:

1. Recibir, analizar, tramitar, procesar y atender las solicitudes que sean turnadas por la UT y registradas a través del sistema electrónico habilitado por los Órganos Garantes, dentro de los plazos establecidos en estos Lineamientos y en estricto apego de la normatividad aplicable, **para lo cual deberá acordar y validar con el Titular del Área a la que pertenece la respuesta que proporcionará a la UT;**
2. Verificar que las respuestas a las solicitudes se pronuncien puntualmente respecto a todas y cada una las peticiones realizadas por el solicitante, de forma accesible, confiable, verificable, veraz, oportuna y en un lenguaje sencillo para cualquier persona, debiendo estar fundadas y motivadas, realizando una búsqueda exhaustiva y razonable de la información solicitada en sus archivos, en las obligaciones de transparencia publicadas en el Portal de Transparencia, en el Portal Principal de esta Secretaría, así como en los comunicados e informes oficiales que haya rendido el titular de esta Secretaría.
3. Verificar que los archivos electrónicos que contengan la documentación y/o información requerida por el solicitante cumplan con el principio de accesibilidad, de tal manera que todas las personas puedan consultarlos, examinarlos y utilizarlos independientemente de sus capacidades técnicas, cognitivas o físicas, por lo que deberán de ofrecerse en un soporte que permita su reutilización por los usuarios y por las máquinas; es decir, presentarse mediante el enfoque de datos abiertos, lo cual implica exportar el conjunto de datos a publicar en formatos estructurados para facilitar el consumo e interpretación, por lo que de ninguna manera podrán contener, claves o cualquier otro tipo de restricción para su acceso.
4. Operar los Sistemas electrónicos habilitados por los Órganos Garantes, así como cualquier otro que los mismos implementen y revisar de manera constante los mismos para el desempeño de las funciones encomendadas;
5. Conocer y dar cumplimiento a la normatividad que, en materia de transparencia, protección de datos personales y archivos resulte aplicable, debiendo capacitarse constantemente en las mismas, en el manejo de los Sistemas Electrónicos y la Plataforma Nacional de Transparencia, para el buen ejercicio de sus funciones;



6. Identificar, organizar, actualizar y validar con el titular de su área administrativa la información requerida por las obligaciones de transparencia que generan y/o poseen en ejercicio de sus facultades, competencias y funciones.
7. Realizar la carga de los formatos homologados en la Plataforma Nacional de Transparencia, una vez que la UT haya supervisado que los mismos den cumplimiento a los criterios para su publicación de conformidad con los lineamientos al efecto aplicables;
8. Atender los requerimientos que realice la UT dentro de los términos solicitados;
9. Apoyar y asesorar a los servidores públicos de su área respecto de la aplicación de la normatividad en las materias de Transparencia y Protección de Datos Personales;
10. Verificar y validar con acuerdo del titular de su área que las propuestas de clasificación de información y declaración de inexistencia, así como las pruebas de daño que al efecto elaboren para ser sometidas ante el Comité de Transparencia, cumplan con la normatividad aplicable, estén debidamente fundadas, motivadas y se consigne en las mismas expresamente los hechos y razonamientos por los cuales se arriba a la conclusión de que el daño que se causa con la difusión de la información es mayor que la utilidad de difundirla, debiendo justificar además los requisitos del artículo 174 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México;
11. Atender el desahogo de todos los requerimientos, trámites y gestiones que se realicen en la materia, dentro del plazo conferido para tales efectos, para lo cual deberá en su caso coordinarse con las demás áreas, en el acopio de información para el cumplimiento de las obligaciones emanadas de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México;
12. Dar cumplimiento a la normatividad aplicable en materia de protección de datos personales.
13. Asistir a las Reuniones de Enlaces y Sesiones de Comité de Transparencia convocadas por la Dirección Ejecutiva de la Unidad de Transparencia;

Sin perjuicio de las anteriores, los enlaces designados en materia de protección de datos personales, tendrán de manera enunciativa más no limitativa las obligaciones siguientes:



1. Conocer y dar cumplimiento a la normatividad que en materia de protección de datos personales y archivos resulte aplicable, debiendo capacitarse constantemente en las mismas, para el buen ejercicio de sus funciones;
2. Atender los requerimientos que realice la UT dentro de los términos solicitados;
3. Apoyar y asesorar a los servidores públicos de su área respecto de la aplicación de la normatividad en la materia de Protección de Datos Personales;
4. Dar cumplimiento a la normatividad aplicable en materia de protección de datos personales.
5. Asistir a las Reuniones de Enlaces;
6. Coordinar con el Responsable del sistema de datos personales y el Responsable de Seguridad, la actualización del documento de seguridad conforme a la normatividad en la materia, así como hacer del conocimiento a los usuarios del sistema las medidas de seguridad y su implementación
7. Actualizar los avisos de privacidad simplificado e integral conforme a la normatividad de la materia vigente, y remitirlos a la Unidad de Transparencia por oficio en el primer mes del año, junto con los formatos en los que se recaben los datos personales con los avisos de privacidad que indistintamente se asienten en los mismos, debidamente actualizado;
8. Mantener actualizados todos los datos requeridos en el Registro Electrónico de Sistemas de Datos Personales (administrado por el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México), como son entre otros los rubros "normatividad aplicable", "Responsable" y "Usuarios";
9. Dar atención y seguimiento hasta su conclusión conjuntamente con la persona responsable del sistema de datos personales y la persona responsable de seguridad, a las verificaciones que realice el Órgano Garante, así como a las denuncias que en su caso se presenten respecto al tratamiento de datos personales.
10. Remitir la información solicitada por la Unidad de Transparencia para la integración del informe anual de protección de datos personales.

Las áreas, deberán implementar las acciones necesarias para cumplir con los requerimientos en los plazos y términos establecidos en los presentes lineamientos.

CIUDAD INNOVADORA
Y DE DERECHOS



Los titulares de las áreas, deberán de verificar que las personas servidoras públicas designadas como enlaces den estricto cumplimiento a las obligaciones antes señaladas, por lo que serán corresponsables de su incumplimiento.

6. DEL TRÁMITE DE LAS SOLICITUDES.

6.1 De la Recepción y Registro de las Solicitudes.

Toda persona por sí o por medio de representante legal, tiene derecho a presentar una solicitud de acceso a la información pública, sin necesidad de acreditar derechos subjetivos, interés legítimo o razones que motiven el requerimiento. Las solicitudes para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante a través de carta poder simple suscrita ante dos testigos, anexando copia de las identificaciones de los suscriptores.

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

El ejercicio de los derechos ARCO de menores de edad se hará a través del padre, madre o tutor y en el caso 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 legislación de la materia.

Tratándose de datos personales concernientes a personas fallecidas, la protección de datos personales no se extingue, por tanto, el ejercicio de Derechos ARCO lo podrá realizar, la persona que acredite tener un interés jurídico o legítimo, el heredero o el albacea de la persona fallecida, de conformidad con las leyes aplicables, o bien exista un mandato judicial para dicho efecto.

Las solicitudes podrán ser presentadas de las siguientes formas:

- De manera verbal ya sea presencial en la UT;
- Vía telefónica (TEL-INFODF);
- Mediante escrito libre o en los formatos aprobados por el Instituto, presentado ante esta Secretaría;
- Por correo electrónico oficial de la UT;
- Por fax, correo postal o telégrafo o
- A través del Sistema Electrónico habilitado para tal efecto; de la Plataforma Nacional de Transparencia, por medio de su sistema de solicitudes de acceso a la información.



Cuando la solicitud se realice verbalmente, el encargado de la Unidad de Transparencia del sujeto obligado que se trate, registrará en un acta o formato la solicitud de información, que deberá cumplir con los requisitos establecidos en la presente Ley, y entregará una copia de la misma al interesado. Cuando la solicitud se realice en escrito libre o mediante formatos, la Unidad de Transparencia registrará en el sistema de solicitudes de acceso a la información la solicitud y le entregará al interesado el acuse de recibo.

Todo el manejo de la información relacionado a solicitudes entre la UT y el Enlace se realizará por los sistemas habilitados por los Órganos Garantes.

Cuando una solicitud se presente ante un área diversa a la UT, aquella deberá remitirla a la UT el mismo día en que la recibió para su correspondiente trámite. En estos casos, los plazos de respuesta empezarán a correr a partir del momento en que la UT reciba la solicitud.

6.2 De la Gestión de Solicitudes.

Una vez recibidas y registradas las solicitudes en el Sistema Electrónico, serán turnadas por la Subdirección de Atención a Solicitudes de Información de la UT, a más tardar al siguiente día hábil de la fecha en que se tengan por presentadas, a la cuenta electrónica del área o áreas que se consideren competentes, a través del sistema electrónico, razón por la cual, es obligación de los Enlaces revisar continuamente su cuenta en el Sistema Electrónico, y en caso de no contar con cuenta en dicho sistema, se turnará por medio del correo electrónico institucional o mediante oficio.

Cualquier anomalía o incidencia en el Sistema Electrónico, debe ser reportada a la UT con sus soportes documentales dentro de las 24 horas siguientes a la que ocurra la misma.

Toda **comunicación y respuesta** a la UT deberá realizarse a través del Sistema Electrónico **antes de las 18:00 horas. Después del horario referido se tendrán por recibidas el día hábil siguiente.**

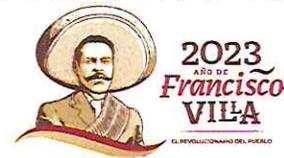
6.3 De la Competencia.

Una vez que el Enlace reciba la solicitud, deberá comunicar a la UT, dentro de los **2 días hábiles siguientes** a la fecha de inicio del trámite, si esa área no es **COMPETENTE** para dar contestación a la solicitud, lo cual deberá fundar y motivar debidamente conforme a las funciones y atribuciones que tiene asignadas, la simple negación de la competencia propia o por afirmación de competencia ajena, no serán suficientes para establecer la incompetencia del área.

Asimismo, deberá informar el nombre del Sujeto Obligado o del área que considera sea competente para atender la solicitud turnada, para lo cual la UT turnará la solicitud en un máximo de un día hábil al área sugerida o en su caso orientará al sujeto obligado competente.

Recibida la contestación de incompetencia por parte del área, la UT deberá corroborar la incompetencia de esta Secretaría para dar respuesta a la solicitud y comunicará al solicitante, el Sujeto Obligado competente para atender su requerimiento, en un plazo no mayor de **3 días hábiles**

Handwritten blue ink marks and signatures on the right margin of the page.



contados a partir de la fecha en que se tenga por presentada la solicitud, debiendo remitir la solicitud a la UT del Sujeto Obligado que corresponda.

En caso de que el área sea competente para atender parcialmente la solicitud, deberá informarlo a la UT dentro del plazo de **3 días hábiles** informando de manera clara y puntual los puntos de la solicitud que atenderá, justificando conforme a lo establecido en este apartado la no competencia e indicando el área o Sujeto Obligado que considere competente de atender los demás puntos de la solicitud.

Si un área omitiera informar a la UT lo expuesto en los párrafos anteriores, se entenderá que es competente para atender la solicitud, por lo que se encontrará obligada a dar la respuesta en los términos establecidos en los presentes Lineamientos.

6.4 De la Prevención.

En caso de considerar necesario realizar una **PREVENCIÓN** al solicitante a efecto de que aclare o precise su solicitud, deberá solicitarla dentro de los **2 días hábiles siguientes** a la fecha de inicio del trámite, a efecto de que la UT analice la viabilidad de la prevención y, en caso de ser procedente, notifique al solicitante en un plazo no mayor a **3 días hábiles** contados a partir de la fecha en que se tenga por presentada la solicitud, para que en un término de **10 días hábiles** contados a partir del día siguiente de su notificación, aclare, precise o complemente su solicitud. En caso de no desahogar dicha prevención, se tendrá por no presentada la solicitud.

En caso de que un área omita informar a la UT de la prevención en el plazo estipulado, se entenderá que la solicitud es clara y precisa; por lo que se encontrará obligada a dar respuesta en los términos establecidos en los presentes lineamientos.

6.5 Del Plazo de Respuesta y Ampliación de Plazo.

De ser competente el área para dar la respuesta requerida por el solicitante, el Enlace deberá remitir la respuesta a la UT a más tardar dentro de los **5 días hábiles siguientes** a la fecha de inicio del trámite, en el caso de ser obligaciones de transparencia, dentro de los **3 días hábiles siguientes** y dentro de los **10 días hábiles siguientes** para las solicitudes de derechos ARCO.

Toda solicitud de información pública, será atendida por la UT, a través de la Subdirección de Atención de Solicitudes de Información, en un plazo no mayor de **9 días hábiles** siguientes a la fecha de inicio del trámite o por desahogada la prevención que en su caso se haya hecho al solicitante de acuerdo a lo establecido en la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México; las solicitudes para el ejercicio de los derechos ARCO deberán ser atendidas dentro de los **15 días hábiles** siguientes a la fecha de inicio del trámite o por desahogada la prevención que en su caso se haya hecho al solicitante de conformidad con lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México; sin embargo, dicho plazo de respuesta deberá ser menor, en cumplimiento a acuerdo emitido por el Jefe de Gobierno publicado el 25 de mayo del 2018 en la Gaceta Oficial de la Ciudad de México, mediante



el cual INSTRUYE A LAS PERSONAS SERVIDORAS PÚBLICAS TITULARES DE LAS DEPENDENCIAS, ÓRGANOS DESCONCENTRADOS, ÓRGANOS POLÍTICO ADMINISTRATIVOS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA DE LA CIUDAD DE MÉXICO, A REALIZAR ACCIONES PARA GARANTIZAR EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y EL DERECHO AL TRATAMIENTO LÍCITO DE DATOS PERSONALES, A LA PROTECCIÓN DE LOS MISMOS, Y EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN, en cual se señala lo siguiente:

...

CUARTO.- El responsable del tratamiento de Datos Personales en cada uno de los Entes de la Administración Pública de la Ciudad de México, deberá observar los Principios de Calidad, Confidencialidad, Consentimiento, Finalidad, Información, Lealtad, Licitud, Proporcionalidad, Transparencia y Temporalidad, así como adoptar las medidas de seguridad necesarias para la protección de datos personales y los sistemas de datos personales.

Los Entes de la Administración Pública de la Ciudad de México, deberán establecer procedimientos sencillos que permitan el ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición, cuyo plazo de respuesta deberá ser menor al previsto en la Ley de la materia.

En ambos casos siempre y cuando la UT cuente con la información entregada por las áreas conforme a los presentes Lineamientos.

Estos plazos podrán ampliarse hasta por **5 días hábiles** más, en el caso de solicitudes de acceso a la información y hasta por **10 días hábiles** más, en las solicitudes para el ejercicio de los derechos ARCO en función del volumen o la complejidad de la información solicitada, debiendo en ambas especificarse las razones fundadas y motivadas que justifican la ampliación, es decir, en qué radica la complejidad para proporcionar la información o cuál es la cantidad de la información que se deberá analizar, razón por la cual no pueda generarse la respuesta en el plazo de los **9 o 15 días hábiles respectivamente** por el área correspondiente, **no podrá invocarse como causales de justificación para la ampliación del plazo, aquellos motivos que supongan negligencia o descuido por parte del área en el desahogo de la solicitud.**

Para que proceda la solicitud de ampliación de plazo, deberá ser solicitada por el área a la UT dentro de los 5 días hábiles siguientes a la fecha de inicio del trámite en el caso de solicitudes de acceso a la información, y de **10 días hábiles** para las solicitudes para el ejercicio de los derechos ARCO.

Las solicitudes en las que se requiera información correspondiente a obligaciones de transparencia, serán atendidas por el área, en un plazo no mayor a **3 días hábiles siguientes** a la fecha de inicio del trámite. **No procede la ampliación del plazo en este tipo de solicitudes.**

El contenido de la respuesta es responsabilidad del Titular del área emisora.

Handwritten signatures and initials in blue ink on the right side of the page.



La UT revisará que las respuestas a las solicitudes se pronuncien puntualmente respecto a todas y cada una de las peticiones realizadas por el solicitante, de forma accesible, confiable, verificable, veraz, oportuna y en un lenguaje sencillo para cualquier persona, estén debidamente fundadas y motivadas, y que no contengan información clasificada como reservada o confidencial, o bien que el área determine sin aprobación del Comité de Transparencia no entregar la información por considerar que sea de dicha naturaleza, en cuyo caso la UT realizará, las sugerencias que considere pertinentes.

La UT preparará la respuesta final y la notificará a través del Sistema Electrónico y en la modalidad elegida por el solicitante.

En caso de que alguna área y/o la UT no proporcionen la respuesta en los términos establecidos en estos Lineamientos, la Dirección Ejecutiva de la Unidad de Transparencia instrumentará constancia de hechos en la que se especifique y detalle la omisión o falta realizada, dándola a conocer a la autoridad correspondiente.

En caso de que los Enlaces remitan una respuesta a la UT, fuera de los plazos establecidos en estos Lineamientos, la UT podrá dar vista a la Contraloría Interna.

Si los Enlaces remiten una respuesta a la UT fuera del plazo conferido por la Ley, la UT deberá gestionar la respuesta y entregarla al solicitante, dando vista a la Contraloría Interna.

En ambos casos, la omisión de respuesta en tiempo y forma, será imputable al Enlace y al titular del área competente.

La UT, a través de la Subdirección de Atención a Solicitudes de Información, elaborará un informe mensual de estos casos, el cual será presentado al titular de la Secretaría.

Handwritten signatures and initials in blue ink, including a large signature at the top right, a vertical line, and several other marks and signatures at the bottom right.



7. DEL CONTENIDO DE LAS RESPUESTAS.

7.1 De la Fundamentación y Motivación.

Todas las respuestas que se proporcionen, independientemente del sentido de las mismas, deberán estar debidamente fundadas y motivadas, en las disposiciones aplicables en la materia (Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, su reglamento, Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, sus lineamientos, Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales en la ciudad de México, Ley General de Archivos), y en la normatividad aplicable al supuesto concreto (Constitución, estatuto de gobierno, Códigos, leyes, reglamentos, reglas generales, lineamientos, manuales, protocolos, etc.).

Asimismo, deberán contener los siguientes requisitos formales:

- a) Hoja con el membrete del área que genere la respuesta.
- b) Número de folio que corresponde a la solicitud, así como la inserción del texto de la misma.
- c) Estar firmada por el titular del área correspondiente que la generó y rubricada por los servidores públicos que la elaboraron, revisaron, dieron su visto bueno y autorizaron la respuesta.
- d) La respuesta emitida deberá ser remitida a través del Sistema Electrónico a la UT.
- e) Los archivos electrónicos que contengan la documentación y/o información requerida por el solicitante cumplan con el principio de accesibilidad, de tal manera que todas las personas puedan consultarlos, examinarlos y utilizarlos independientemente de sus capacidades técnicas, cognitivas o físicas, por lo que cuenta deberán de ofrecerse en un soporte que permita su reutilización por los usuarios y por las máquinas; es decir, presentarse mediante el enfoque de datos abiertos, lo cual implica exportar el conjunto de datos a publicar en formatos estructurados para facilitar el consumo e interpretación, por lo que de ninguna manera podrán contener, claves o cualquier otro tipo de restricción para su acceso.

7.2 De las Solicitudes que Requieran la Realización de un Trámite.

La UT está obligada a orientar en forma sencilla y comprensible a toda persona sobre los trámites y procedimientos que deben efectuarse para solicitar información, indicando las autoridades o instancias competentes, la forma de realizarlos, la manera de llenar los formularios que se requieran, así como de las instancias ante las que se puede acudir a solicitar orientación o para formular quejas, consultas o reclamos sobre la prestación del servicio o sobre el ejercicio de las funciones o competencias a cargo de los servidores públicos de que se trate.



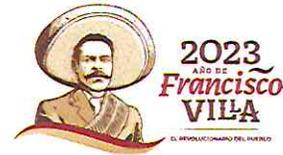
En caso de que la respuesta del área correspondiente, oriente al solicitante para que obtenga su información a través de algún trámite establecido, su respuesta deberá apegarse a lo dispuesto en el artículo 52 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y el artículo 201 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

7.3 Del Procesamiento de la Información.

En términos de la normatividad aplicable, las áreas competentes deberán dar atención puntual a cada solicitud, y dar acceso a las personas respecto de la información en posesión de la Secretaría y a la defensa de sus derechos ARCO.

Las áreas deberán entregar la información solicitada en el estado en el que se encuentre en sus archivos, es decir, la atención de una solicitud no debe implicar procesamiento de la información, ni el presentarla conforme al interés particular del solicitante.

Handwritten signatures and marks in blue ink on the right side of the page.



8. DE LA CLASIFICACIÓN DE INFORMACIÓN Y DE LA INEXISTENCIA.

8.1 De las Modalidades de Clasificación de Información.

La información puede ser clasificada en dos modalidades:

- Reservada
- Confidencial

Información RESERVADA.

Definición	Información pública que se encuentre temporalmente sujeta a alguna de las excepciones previstas en la Ley.
Causales de Reserva	Las establecidas en el Artículo 183 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Plazo de la clasificación	No se podrá divulgar la información clasificada como reservada, por un periodo de hasta tres años contados a partir de la fecha en que se clasificó la información por el Comité de Transparencia de esta Secretaría. El periodo de reserva podrá ser excepcionalmente renovado hasta por dos años más.

Información CONFIDENCIAL.

Definición	La que contiene datos personales concernientes a una persona identificada o identificable. Se considera como información confidencial: los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos, la protegida por la legislación en materia de derechos de autor o propiedad intelectual. Asimismo, será información confidencial aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.
Causales de Información Confidencial	Las establecidas en el Artículo 186 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.
Plazo de la clasificación	La información confidencial no está sujeta a temporalidad alguna, por lo que tendrá ese carácter de manera indefinida y solo podrán tener acceso a ella los titulares de la misma, sus representantes y las personas servidoras públicas facultadas

[Handwritten signatures and initials in blue ink on the right margin]



para ello, por lo que queda estrictamente prohibida su difusión, salvo las excepciones contempladas en la Ley.

8.2 Del Procedimiento para la Clasificación de la Información y Versiones Públicas.

Si un área considera que la información solicitada debe ser clasificada en cualquiera de sus dos modalidades, reservada o confidencial, **dentro de los 3 días hábiles siguientes a la fecha en que sea turnada la solicitud por parte de la UT, deberá remitir un oficio a la UT** en el que funde y motive la clasificación de información para la aprobación del Comité de Transparencia con los siguientes elementos:

1. Área que genera, administra o detenta la información;
2. Las hipótesis de excepción previstas en la ley, en la que se encuadre la información materia de la clasificación;
3. Si se trata de información clasificada en la modalidad de reservada deberá acompañar al oficio la prueba de daño en el formato correspondiente, firmada en todas sus hojas por el titular del área en la que funde y motive la clasificación de información conforme a lo señalado en las tres hipótesis del artículo 174 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México,
4. En el caso de que la información sea clasificada en la modalidad de confidencial se deberá incluir los datos personales o la información confidencial de los cuales se solicita su clasificación y fundar y motivar conforme a la Ley de Transparencia antes citada y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.
5. Si de la información que se requiere se desprende que del documento solo una parte será clasificada en cualquiera de sus modalidades, el área solicitara también la elaboración de la Versión Pública del documento en el que se encuentra la información, la cual deberá de estar apegada a los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas y demás normatividad aplicable.

En dicho oficio, deberá solicitarse que, con fundamento en el artículo 216 de la Ley, se convoque al Comité de Transparencia para que se someta a su consideración la propuesta de clasificación correspondiente.

Asimismo, deberá incluirse, copia simple de la información o los documentos que serán sujetos de clasificación para ser analizada la información por los miembros del Comité de Transparencia de esta Secretaría, o, en su defecto y sólo en caso de que por el volumen esto sea complejo o no pueda ser reproducida, deberá acompañar una muestra de la información materia de la clasificación y la

[Handwritten signatures and marks in blue ink on the right margin]



manifestación expresa e inequívoca de que la información existe y que se encuentra en custodia del área, dicha documentación, quedará una vez analizada por la UT y el Comité bajo el resguardo del área que la presentó.

Las áreas competentes para atender las solicitudes, a través de su enlace designado, deberán enviar a la UT, cuando así proceda, la prueba de daño en el formato correspondiente, debidamente firmada en todas sus hojas por su titular, así como los argumentos lógico - jurídicos para fundar y motivar la clasificación de la información, en los que se justifique que:

- I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público;
- II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y
- III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

La carga de la prueba para justificar toda negativa de acceso a la información, por actualizarse cualquiera de los supuestos de reserva previstos en la Ley, corresponderá a las áreas.

Actividad	Forma
Solicitud de Comité de Transparencia	Las áreas después de haber recibido una solicitud de acceso a la información pública, en la que se determine que la información requerida actualice alguno de los supuestos de reserva o confidencial, remitirá a la UT, solicitud de Comité debidamente fundada y motivada
En caso de solicitar clasificación de la información en su modalidad de reservada	El área en su oficio de solicitud de Comité de Transparencia, anexara prueba de daño conforme a lo establecido en el artículo 174 de la Ley de Transparencia Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México. Además de remitir su solicitud de manera oficial, deberán remitirla vía correo electrónico a la Subdirección de Transparencia.
En caso de solicitar clasificación en su modalidad de confidencial	El área en su oficio de solicitud de Comité de Transparencia, incluirá cuales son los datos personales o la información confidencial de los cuales se solicita su clasificación.

Handwritten signatures and initials in blue ink on the right margin.



	Además de remitir su solicitud de manera oficial, deberán remitirla vía correo electrónico a la Subdirección de Transparencia.
Versión Pública	En ambos casos de ser procedente se remitirá la Versión Pública con apego a los Lineamientos generales en materia de clasificación y desclasificación de información, así como para la elaboración de versiones públicas. Vigentes.

[Handwritten signatures and initials in blue ink]

Una vez recibido el oficio del área correspondiente con sus soportes documentales, la Subdirección de Transparencia deberá revisar y analizar la propuesta de clasificación y, en caso de ser procedente, deberá convocar al Comité para que sesione a la brevedad posible y se pronuncie respecto de la clasificación.

Si el oficio por el que se solicita sesión del Comité de Transparencia no cubre con todos los requisitos establecidos en estos lineamientos y la normatividad aplicable, no será presentado ante el Comité, quedando a entera responsabilidad del área solicitante.

Los casos de excepción al derecho de acceso a la información y a la protección de datos personales se encuentran regulados, por lo que no podrá clasificarse la información que no se encuentre dentro de los supuestos que expresamente señala la normatividad aplicable; en ningún caso se podrán emitir acuerdos generales que clasifiquen información como reservada, aún y cuando guarden cierta analogía con casos precedentes, pues la misma puede únicamente ser clasificada bajo los supuestos siguientes:

- Se reciba una solicitud de acceso a la información;
- Se determine mediante resolución de la autoridad competente o
- Se generen versiones públicas para dar cumplimiento a las obligaciones de transparencia previstas en la Ley y demás ordenamientos aplicables.

[Large handwritten signature and initials in blue ink]

El Comité podrá confirmar, modificar o revocar la clasificación, así como aprobar las versiones públicas de conformidad con los lineamientos aplicables en las que se teste la información clasificada.

Una vez que el Comité de Transparencia aprueba la clasificación el área deberá remitir su respuesta a la UT en los plazos establecidos en los presentes lineamientos.

En los casos de consulta directa, las áreas solicitarán sesión de Comité Transparencia, para lo cual se deberá solicitar mediante oficio a la UT, sustentado en los artículos 90 fracciones I y IV, 207 y 213 de la Ley, acompañando al mismo la propuesta de lineamientos para llevar a cabo la diligencia para la consulta directa de la información, los cuales deberán ser acordes con lo señalado en los



Lineamientos generales en materia de clasificación y desclasificación de información, así como para la elaboración de versiones públicas.

Derivado de la clasificación de la información y la entrega de versiones públicas, las áreas deberán asegurarse que los expedientes y documentos clasificados cumplan con los requisitos que se establecen en los Lineamientos generales en materia de clasificación y desclasificación de información, así como para la elaboración de versiones públicas, conforme a lo siguiente:

EN EL CASO DE LA VERSIÓN PÚBLICA DE DOCUMENTOS ELECTRÓNICOS O FÍSICOS CLASIFICADOS COMO CONFIDENCIALES, DEBERÁ DE CONTENER LOS SIGUIENTES REQUISITOS:

TESTADO, (PALABRAS, PÁRRAFOS o RENGLONES según sea el caso) **CONSISTENTES EN:** (ejemplo NOMBRE, FIRMA, NÚMERO DE EMPLEADO o etc.), **EN VIRTUD DE SER** (INFORMACIÓN CONFIDENCIAL) **CON FUNDAMENTO EN LO DISPUESTO EN EL ARTÍCULO (186) DE LA LEY DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO; FECHA DE APROBACIÓN DE LA ELABORACIÓN PÚBLICA APROBADA POR EL COMITÉ; FECHA DE LA ELABORACIÓN DE LA VERSIÓN PÚBLICA; SEÑALAR LAS PERSONAS O INSTANCIAS AUTORIZADAS PARA ACCEDER A LA INFORMACIÓN CLASIFICADA** (ejemplo NOMBRE DE LA UNIDAD QUE DETENTA O POSEE LA INFORMACIÓN CLASIFICADA Y TITULAR DE LOS DATOS PERSONALES), APROBÁNDOSE LA ELABORACIÓN DE VERSIÓN PÚBLICA, CON FUNDAMENTO EN EL ARTÍCULO 180 DE LA CITADA LEY DE TRANSPARENCIA Y DE ACUERDO A LOS NUMERALES 50,52, 61 Y 62 DE LOS LINEAMIENTOS GENERALES EN MATERIA DE CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN ASÍ COMO PARA LA ELABORACIÓN DE VERSIONES PÚBLICAS.

EN EL CASO DE LA VERSIÓN PÚBLICA DE DOCUMENTOS O EXPEDIENTES ELECTRÓNICOS O FÍSICOS QUE HAYAN SIDO CLASIFICADOS COMO RESERVADOS, DEBERÁ DE CONTENER CON EL SIGUIENTE FORMATO:

Sello oficial o logotipo de la Secretaría	Fecha de clasificación	Se anotará la fecha en la que el Comité de Transparencia confirmó la clasificación del documento o expediente, en su caso.
	Área	Se señalará el nombre del área del cual es titular quien clasifica.

Handwritten signatures and initials in blue ink on the right margin.



	<p>Información reservada</p>	<p>Se indicarán las partes o páginas del documento que se clasifican como reservadas, o, en su caso, se precisará que se ha reservado El documento o expediente en su totalidad.</p>
	<p>Periodo de reserva</p>	<p>Se anotará el número de años o meses por los que se mantendrá reservado el documento, el expediente o, en su caso, las partes o secciones reservadas.</p>
	<p>Fundamento legal</p>	<p>Se señalará el nombre del ordenamiento, el o los artículos, fracción (es), párrafo(s) con base en los cuales se sustente la reserva.</p>
	<p>Ampliación del periodo de reserva</p>	<p>En caso de haber solicitado la ampliación del periodo de reserva originalmente establecido, se deberá anotar el número de años o meses por los que se amplía la reserva.</p>

[Handwritten notes and signatures in blue ink on the right margin of the table, including a large 'T' and several illegible signatures.]

[Handwritten signatures and initials in blue ink at the bottom right of the page.]



	Rúbrica del Titular de área	Rúbrica autógrafa o firma digital de quien clasifica.
	Fecha de desclasificación	Se anotará la fecha en que se desclasifica el documento.
	Rubrica y cargo del servidor público	Rúbrica autógrafa o firma digital de quien desclasifica.

Los documentos que integren un expediente reservado en su totalidad no deberán marcarse en lo individual.

Una vez desclasificados los expedientes, si existieren documentos que tuvieran el carácter de reservados deberán permanecer o ser marcados.

8.3 De la Ampliación del Plazo de Reserva.

Excepcionalmente las áreas podrán ampliar el periodo de reserva de la información con la aprobación del Comité de Transparencia, hasta por un plazo de dos años adicionales, siempre y cuando se justifique que subsisten las causas que dieron origen a su clasificación, mediante la aplicación de una nueva prueba de daño.

Para los casos en que esté por expirar el plazo de clasificación de la información ya con ampliación y su publicación pueda ocasionar la destrucción o inhabilitación de la infraestructura de carácter estratégico para la provisión de bienes o servicios públicos y que a juicio del área deba ampliarse nuevamente el periodo de reserva de la información, deberá de solicitar a la UT **con un plazo de anticipación de cuatro meses al vencimiento del plazo de reserva**, para que el Comité de Transparencia esté en posibilidades de realizar la solicitud de ampliación ante el Instituto.

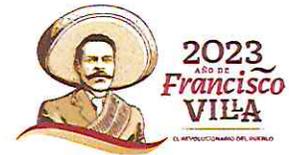
En ambos supuestos de ampliación se deberá de seguir el procedimiento para la clasificación de la información señalado en los presentes lineamientos.

8.4 De los Índices de Información Previamente Clasificada como Reservada.

Los titulares de las áreas de la Secretaría deberán elaborar semestralmente un índice en formatos abiertos, de la información clasificada como reservada por el Comité de Trasparencia, el cual deberá contener lo siguiente:

- I. El área que generó, obtuvo, adquirió, transformó y/o conserve la información;
- II. El nombre del documento;
- III. Fracción del numeral séptimo de los presentes lineamientos que da origen a la reserva;
- IV. La fecha de clasificación;

[Handwritten signatures and initials in blue ink on the right margin]



- V. El fundamento legal de la clasificación;
- VI. Razones y motivos de la clasificación;
- VII. Señalar si se trata de una clasificación completa o parcial;
- VIII. En caso de ser parcial, las partes del documento que son reservadas;
- IX. En su caso, la fecha del acta en donde el Comité de Transparencia confirmó la clasificación;
- X. El plazo de reserva y si se encuentra o no en prórroga;
- XI. La fecha en que culmina el plazo de la clasificación;
- XII. Las partes o secciones de los expedientes o documentos que se clasifican; y
- XIII. El índice de expedientes clasificados como reservados deberá indicar únicamente la información cuya reserva se encuentre vigente al momento de su elaboración, debiéndose eliminar del índice aquella que haya sido desclasificada.

Dicho índice se deberá de actualizar de manera semestral y hacer del conocimiento al Comité de Transparencia, solicitando mediante a oficio a la UT su publicación en el Portal de Transparencia de la Secretaría y en la Plataforma Nacional de Transparencia, la cual deberá de ser dentro de los primeros días hábiles de los meses de enero y julio de cada año, según corresponda en formatos abiertos. En ningún caso el índice será considerado como información reservada.

Será responsabilidad de los titulares de las áreas el custodiar y conservar la documentación e información clasificada, conforme a las disposiciones legales aplicables.

8.5 De la Inexistencia de Información y de Datos Personales.

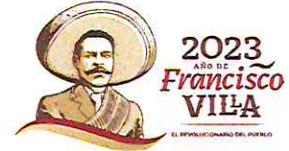
Se presume que la información existe en la medida que deriva del ejercicio, facultades, competencias o funciones que los ordenamientos jurídicos aplicables otorgan a la Secretaría, dentro de los plazos y conforme a la clasificación, establecidos en la normatividad en materia de Archivos.

Los Enlaces de las áreas, deberán informar a la UT dentro de los **3 días hábiles siguientes** contados a partir del ingreso de la solicitud, respecto de la inexistencia de la información solicitada.

Es indispensable para su procedencia que en el oficio se especifique con claridad y detalle las acciones que el área implementó para buscar de manera exhaustiva la información requerida en la solicitud, se expongan las razones y/o motivos por las cuales en el caso particular y previa acreditación, no ejerció dichas facultades, competencias o funciones que justifiquen la inexistencia, así como los nombres de los funcionarios públicos que se encuentran como responsables de la guarda y custodia de la información.

Adicionalmente, en el oficio deberá solicitarse la intervención del Comité de Transparencia para que, en el ejercicio de sus funciones y de conformidad con la normatividad aplicable, analice el caso y tome

[Handwritten signatures and initials in blue ink on the right margin]

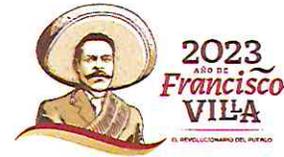


las medidas necesarias para localizar la información y resolver en consecuencia, pronunciándose respecto de la declaratoria de inexistencia.

El Comité de Transparencia expedirá una resolución en la que confirme la **inexistencia** del documento, o bien de los datos personales según sea el caso y de ser procedente, ordenará siempre que sea materialmente posible se genere la información, en caso en que esta tuviera que existir en la medida que deriva del ejercicio de sus facultades, competencias o funciones, o que previa acreditación de la imposibilidad de su generación exponga las razones por las cuales en el caso particular no ejerció dichas facultades, competencias o funciones, dicha resolución del Comité deberá contener los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y señalará al servidor público responsable de contar con la misma. En cualquiera de los supuestos referidos, el área competente deberá elaborar la respuesta al solicitante en la que le informe los términos en los que el Comité se pronunció y la entregará a la UT, para que ésta a su vez la notifique al solicitante. El Comité de Transparencia notificará al Órgano Interno de Control de la Secretaría, la declaratoria de inexistencia, quien en su caso deberá iniciar el procedimiento de responsabilidad administrativa que corresponda.

Para que el Comité realice la declaración de inexistencia de un documento, deberán participar en la sesión los titulares de las áreas competentes en el asunto.

Handwritten signatures and initials in blue ink on the right side of the page.



9. DE LAS OBLIGACIONES DE TRANSPARENCIA.

Con la finalidad de transparentar y publicitar los actos realizados por la Secretaría en el ejercicio de sus funciones, y en cumplimiento a la Ley, toda la información considerada como obligaciones de transparencia, deberá conservarse impresa para consulta directa de los particulares, difundirse y mantenerse actualizada a través de los respectivos medios electrónicos, en el portal de Transparencia de esta Secretaría y en la Plataforma Nacional de Transparencia. Al inicio de cada ejercicio, la UT difundirá el calendario de actualización que deberán atender las áreas durante el ejercicio notificado.

Para la actualización de las obligaciones de transparencia, todas las áreas deberán entregar a la UT la información que sea de su competencia en los formatos debidamente requisitados con apego a los criterios establecidos en los Lineamientos vigentes, o en cualquier otra normatividad que para tales efectos establezcan los Órganos Garantes.

Será obligación de los titulares de las áreas concentradoras de información para el cumplimiento de las obligaciones de transparencia, coordinarse con las otras áreas no concentradoras en el llenado de los formatos respectivos, debiendo remitir las primeras a la UT el o los formatos debidamente llenados de forma impresa y electrónica para su validación y publicación en el Portal de Transparencia, por lo que al inicio de cada ejercicio, los titulares de las áreas deberán atender los plazos establecidos para la actualización de las obligaciones de transparencia establecidos en los lineamientos antes referidos.

El enlace designado deberá integrar la información que de acuerdo a sus atribuciones sean competencia de su área, validar la misma con su titular y realizar su carga en el Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT) una vez que la UT haya realizado la supervisión de los formatos y que estos cumplan con los criterios establecidos en la normatividad de la materia.

La UT asignará las claves de acceso y nombres de usuarios para la carga de la información por artículo y/o fracción al titular del área, siendo su responsabilidad el resguardar y adoptar las medidas de seguridad necesarias para evitar su mal uso, sustracción, divulgación o alteración de la información contenida en la Plataforma Nacional de Transparencia.

La UT requerirá por oficio a los titulares de las áreas, los formatos debidamente requisitados con las obligaciones de transparencia actualizadas y la información verificada y validada que sean de su competencia, los cuales deberán de ser remitidos mediante oficio y CD para la supervisión de la UT, en la fecha que ésta indique para tales efectos y para que en su caso esta proceda a su publicación en el Portal de Transparencia de esta Secretaría.

La responsabilidad última del contenido de la información es exclusiva de cada una de las áreas que la proporcionan, por lo que será obligación de sus titulares actualizar y validar la información de las

[Handwritten signatures and initials in blue ink on the right margin]



obligaciones de transparencia en la sección correspondiente del Portal de Transparencia y en la Plataforma Nacional de Transparencia.

Las versiones públicas que elaboren las áreas para dar cumplimiento a las obligaciones de transparencia, deberán apegarse a lo establecido por los **Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas**, y deberán ser remitidas mediante oficio a la UT para su aprobación por el Comité de Transparencia por lo menos 15 días hábiles antes al vencimiento de los plazos establecidos por la normatividad aplicable para su publicación.

Será obligación de los titulares de cada área así como de sus enlaces designados atender el Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT), generar, mantener activa y revisar permanentemente la cuenta de correo electrónico oficial de su área asignada para tales efectos, a fin de mantener comunicación para el cumplimiento de las obligaciones de transparencia, además de establecer en su área, los procedimientos necesarios para identificar, organizar actualizar y validar la información que generen y/o poseen en ejercicio de sus facultades y publicarla en la Plataforma Nacional de Transparencia, observando que la información cumpla con los atributos de: calidad de la información, accesibilidad, sea veras, confiable, oportuna, congruente, integra, reutilizable, accesible, actual, comprensible verificable y gratuita.

La Unidad de Transparencia tendrá la responsabilidad de recabar la información generada, validada, organizada y requisitada en los formatos de Excel correspondientes por las áreas de esta Secretaría y conforme a la normatividad aplicable, únicamente para supervisar que cumpla con los criterios establecidos en los Lineamientos vigentes o en cualquier otra normatividad que establezcan los Órganos Garantes, para su publicación en el Portal de Transparencia de esta Secretaría.

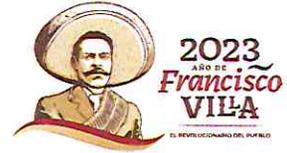
En el caso de que la información remitida por el área competente a la UT, se apegue a la normatividad aplicable para su publicación, esta última notificará a través de la cuenta de correo generada para tales efectos al titular del área, así como a su enlace, para que éste último proceda a cargar la información en el Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT) asegurándose que el total de registros cargados en el Sistema de Obligaciones del Portal de Obligaciones de Transparencia SIPOT, corresponda con el total de registros publicados en el Portal de Transparencia de esta Secretaría, debiendo remitir por oficio a la UT el comprobante de término de la carga correspondiente que emite dicho sistema, al día siguiente de su publicación.

Para el caso de que la información remitida por el área competente no cumpla con los criterios aplicables señalados para su publicación, esta deberá de subsanar las observaciones que sobre la misma realice la UT de manera inmediata.

9.1 De la Transparencia Proactiva.

Cada una de las áreas de esta Secretaría a través de su enlace designado, deberá de proporcionar a la UT en los formatos que más convengan al público al que va dirigida, la información de interés público

Handwritten signatures and initials in blue ink on the right margin of the page.



6

conforme a los Lineamientos para determinar los catálogos y publicación de información de interés público; y para la emisión y evaluación de políticas de transparencia proactiva y conforme a las políticas de transparencia que emita el Instituto, para los efectos de publicarla y actualizarla en los respectivos sitios de internet de esta Secretaría.

La información que se publique, como resultado de las políticas de transparencia proactiva, deberá permitir la generación de conocimiento público útil, para disminuir asimetrías de la información, mejorar los accesos a trámites y servicios, optimizar la toma de decisiones de autoridades o ciudadanos y deberá tener un objeto claro enfocado en las necesidades de sectores de la sociedad determinados o determinables.

[Firma]

[Firma]

[Firma]

[Firma]

[Firma]

[Firma]



10. DE LA ATENCIÓN A LAS VERIFICACIONES Y DENUNCIAS.

10.1 Del Procedimiento de Verificación a las Obligaciones de Transparencia

La UT, notificará al día siguiente de su recepción a los titulares de las áreas competentes, los requerimientos, recomendaciones u observaciones que formulen los Órganos Garantes con motivo de la verificación a las obligaciones de transparencia, para que sean subsanadas de manera inmediata, debiendo informar mediante oficio a la UT de su cumplimiento, acompañando en CD los formatos materia de la verificación debidamente requisitados, a efecto de que la UT realice la supervisión del cumplimiento, procediendo a la carga de la información en el Portal de Transparencia de esta Secretaría y así estar en posibilidad de informar del citado cumplimiento al Órgano Garante respectivo.

Una vez realizada la carga de la información motivo de la verificación en el Portal de Transparencia, la UT notificará al área competente para que esta cargue de manera inmediata la información en el Sistema de Portales de Obligaciones de Transparencia de la Plataforma Nacional de Transparencia (SIPOT), conforme a los presentes Lineamientos.

En caso de que la UT sea notificada por los Órganos Garantes de la existencia de un incumplimiento total o parcial de los requerimientos, recomendaciones u observaciones, la UT al día siguiente de su recepción notificará al superior jerárquico del servidor público responsable de dar cumplimiento, para que de manera inmediata atienda los mismos, debiendo informar a la UT de su cumplimiento, conforme a lo señalado en los párrafos anteriores.

Será responsabilidad del área competente el incumplimiento parcial o total de la resolución del Órgano Garante.

10.2 Del Procedimiento de Verificación a los Principios y Disposiciones Contenidas en la LPDPPSOCDMX y demás ordenamientos derivados de esta.

La verificación podrá iniciarse:

- I. De oficio cuando el Instituto cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes;
- II. Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la Ley y demás normativa aplicable;
- III. Por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la Ley y demás disposiciones que resulten aplicables en la materia;



- IV. Para verificar el cumplimiento de los principios, el tratamiento de los datos personales y la gestión de los sistemas de datos personales en posesión del responsable, para tal efecto el Instituto presentará un programa anual de verificación.

La denuncia establecida en la fracción II referida, se resolverá de conformidad con el Procedimiento que para tal efecto emita el Instituto.

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

El procedimiento de verificación concluirá con la resolución que emita el Instituto, en la que se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.

10.3 De las Denuncias por Incumplimiento a las Obligaciones de Transparencia.

Los titulares de las áreas competentes deberán atender las denuncias que por incumplimiento a las obligaciones de transparencia se presenten, y dar cumplimiento a las resoluciones que con motivo de estas emitan los Órganos Garantes.

Notificada que sea al titular del área competente la denuncia presentada, este deberá de remitir mediante oficio y por correo institucional a la UT al día hábil siguiente de su recepción, un informe con justificación respecto de los hechos o motivos de la denuncia, así como los informes complementarios que en su caso sean solicitados por los Órganos Garantes.

Una vez notificada la resolución al titular del área competente, éste deberá dar cumplimiento a la misma e informar sobre su cumplimiento a la UT **dentro del término de 5 días hábiles, contados a partir del día siguiente en el que le fue notificada la misma, para que la UT notifique al Órgano Garante su cumplimiento.**

Notificada que sea a la UT por los Órganos Garantes de la existencia de un incumplimiento total o parcial a la resolución emitida por estos últimos, la UT al día siguiente de su recepción notificará al superior jerárquico del servidor público responsable de dar cumplimiento, **para que en un plazo de 3 días hábiles dé cumplimiento a la resolución y notifique a la UT, para que esta esté en posibilidad de informar al Órgano Garante el cumplimiento.**

Será responsabilidad del área competente el incumplimiento parcial o total de la resolución del Órgano Garante.



11. DE LOS RECURSOS DE REVISIÓN.

Procede el recurso de revisión de conformidad con la **Ley**, por cualquiera de las siguientes causas:

- I. La clasificación de la información;
- II. La declaración de inexistencia de información;
- III. La declaración de incompetencia por el sujeto obligado;
- IV. La entrega de información incompleta;
- V. La entrega de información que no corresponda con lo solicitado;
- VI. La falta de respuesta a una solicitud de acceso a la información dentro de los plazos establecidos en la ley;
- VII. La notificación, entrega o puesta a disposición de información en una modalidad o formato distinto al solicitado;
- VIII. La entrega o puesta a disposición de información en un formato incomprensible y/o no accesible para el solicitante;
- IX. Los costos o tiempos de entrega de la información;
- X. La falta de trámite a una solicitud;
- XI. La negativa a permitir la consulta directa de la información;
- XII. La falta, deficiencia o insuficiencia de la fundamentación y/o motivación en la respuesta, o
- XIII. La orientación a un trámite específico.

Procede el recurso de revisión de conformidad con la **LPDPPSOCDMX**, por cualquiera de las siguientes causas:

- I. La inexistencia de los datos personales;
- II. La declaración de incompetencia por el sujeto obligado;
- III. La entrega de datos personales incompletos;
- IV. La entrega de datos personales que no correspondan con lo solicitado;
- V. La negativa al acceso, rectificación, cancelación u oposición de datos personales;
- VI. La falta de respuesta a una solicitud de acceso, rectificación, cancelación u oposición de datos personales, dentro de los plazos establecidos en la presente ley;

[Handwritten signatures and marks in blue ink on the right margin]



- VII. La entrega o puesta a disposición de datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;
- VIII. Los costos de reproducción o tiempos de entrega de los datos personales;
- IX. La obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos personales, a pesar de que fue notificada la procedencia de los mismos; o
- X. La falta de trámite a una solicitud para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos personales.

En ambos casos el recurso de revisión deberá presentarse dentro de los quince días hábiles contados a partir de la notificación de la respuesta a la solicitud. En caso de que no se haya emitido respuesta, será a partir del vencimiento del plazo para la entrega de la respuesta a la solicitud.

11.1 En materia de acceso a la información:

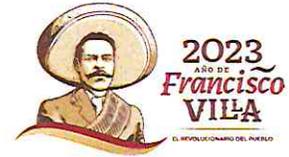
La respuesta de esta Secretaría derivada de una resolución a un recurso de revisión **en materia de acceso a la información** que proceda por los supuestos indicados en las fracciones III, VI, VIII, IX y XI del artículo 234 de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, serán susceptibles de ser impugnadas de nueva cuenta, mediante recurso de revisión ante los Órganos Garantes.

Se considerará falta de respuesta por el área competente en los siguientes supuestos:

- I. Cuando concluido el plazo establecido en los presentes lineamientos para atender una solicitud de información pública, no haya emitido ninguna respuesta;
- II. Cuando haya señalado que se anexó una respuesta o la información solicitada, en tiempo, sin que lo haya acreditado;
- III. Al dar respuesta materialmente emita una prevención o ampliación de plazo, y
- IV. Cuando en su respuesta al recurrente manifieste que por cargas de trabajo o problemas internos no está en condiciones de dar respuesta a la solicitud de información.

11.2 De las manifestaciones, pruebas y alegatos.

En ambos casos (**derecho de acceso a la información y ejercicio de los derechos ARCO**), una vez admitido por el Órgano Garante el recurso de revisión, ordenará a la Secretaría que dentro de los **siete días hábiles siguientes**, manifieste lo que a su derecho convenga respecto del acto o resolución recurrida, que le sirvieron de base para la emisión de dicho acto, se ofrezcan las pruebas o alegatos que considere pertinentes.



Una vez que el Órgano Garante notifique a la UT el acuerdo a través del cual se admitió el recurso de revisión en contra de la respuesta emitida, ésta última notificará al área competente a más tardar el día siguiente de su recepción la interposición del recurso de revisión en contra de su respuesta y requerirá las manifestaciones, pruebas o alegatos correspondientes, por correo electrónico y por oficio.

Con la finalidad de que la UT consolide los argumentos para una mejor defensa de los intereses de la Secretaría, el área deberá remitirle dentro de los **3 días hábiles siguientes a la notificación del recurso interpuesto**, las manifestaciones, pruebas o alegatos respectivos, para que la UT, los haga valer ante el Órgano Garante dentro del plazo establecido por la Ley.

Las manifestaciones, pruebas o alegatos que las áreas entreguen a la UT, deberán justificar, fundamentar y motivar la respuesta emitida y deberá refutar todos y cada uno de los agravios expuestos por el recurrente, anexando, para el efecto, copia de todos los documentos que acrediten la legalidad de la respuesta entregada al solicitante.

Las manifestaciones referidas en el punto anterior, deberán estar fundadas en la normatividad aplicable.

El área podrá presentar, si lo considera pertinente, una respuesta complementaria al solicitante recurrente en la que realice precisiones o entregue información adicional respecto de la respuesta original, la cual deberá ser entregada a la UT junto con las manifestaciones, pruebas o alegatos respectivos.

11.3 Del cumplimiento de las resoluciones.

Una vez decretado el cierre de la instrucción, el Órgano Garante emitirá la resolución correspondiente, en la que se establezcan los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución.

El Pleno del Órgano Garante, en la resolución que dicte, podrá desechar el recurso, sobreseer el mismo, confirmar la respuesta, modificar la respuesta emitida; revocar la respuesta del sujeto obligado u ordenar que se atienda la solicitud.

Cuando el Instituto notifique la resolución a esta Secretaría, la UT hará extensiva la notificación por oficio al área administrativa competente, adjuntando copia de la resolución para que dé cumplimiento a lo ordenado por el Órgano Garante y remita la respuesta correspondiente a la UT en el plazo estipulado en el oficio de notificación, plazo que podrá ser excepcionalmente ampliado en consideración de las circunstancias especiales del caso, debiendo estar debidamente fundado y motivado y ser solicitado por el área al día hábil siguiente de ser notificado el requerimiento.

La UT deberá informar al Instituto respecto del cumplimiento dado a su resolución, en el plazo que se indique en la misma.

En caso de incumplimiento de la resolución, el Instituto notificará al superior jerárquico del responsable de dar cumplimiento a fin de que ordene el cumplimiento en un plazo que no excederá de **5 días**

Handwritten signatures and initials in blue ink on the right margin of the page.



hábiles, determinando las medidas de apremio o sanciones, según correspondan que deberán imponerse o las acciones procedentes que deberán aplicarse.

h

[Firma manuscrita]

[Firma manuscrita]

[Firma manuscrita]

[Firma manuscrita]



12. DE LOS RECURSOS DE INCONFORMIDAD.

12.1 En materia de acceso a la información.

Procede el recurso de inconformidad en contra de las resoluciones emitidas por el Órgano Garante que:

- I. Confirмен o modifiquen la clasificación de la información, o
- II. Confirмен la inexistencia o negativa de información.

12.2 Respecto del Ejercicio de los Derechos ARCO.

Procede el recurso de inconformidad en contra de las resoluciones emitidas por el Órgano Garante que:

- I. Clasifiquen los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
- II. Determinen la inexistencia de datos personales, o
- III. Declaren la negativa de datos personales, es decir:
 - a) Se entreguen datos personales incompletos;
 - b) Se entreguen datos personales que no correspondan con los solicitados;
 - c) Se niegue el acceso, rectificación, cancelación u oposición de datos personales;
 - d) Se entregue o ponga a disposición datos personales en un formato incomprensible;
 - e) El titular se inconforme con los costos de reproducción, envío, o tiempos de entrega de los datos personales, o
 - f) Se oriente a un trámite específico que contravenga lo dispuesto por el artículo 54 de la presente Ley.

En ambos casos el recurso de inconformidad se sustanciará atendiendo a lo dispuesto por la Ley General aplicable respectiva.

[Handwritten signatures and marks in blue ink on the right margin]



13. DE LA CAPACITACIÓN Y DE LA CULTURA DE LA TRANSPARENCIA.

13.1 De la Capacitación a los Servidores Públicos.

En atención a las obligaciones que en materia de capacitación de los servidores públicos, se encuentra contenida en la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, toda las personas servidoras públicas de la Secretaría deberán estar capacitadas de acuerdo a los programas de capacitación que se implementen por los Órganos Garantes, la UT y el Comité de Transparencia.

Además deberán estar capacitados en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y demás normatividad que resulte aplicable, todas aquellas que en el ejercicio de sus funciones traten datos personales o funjan como Responsables, Responsables de Seguridad o usuarios de alguno de los sistemas de datos personales de esta Secretaría.

Para realizar los cursos introductorios de la "Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México", la "Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México", así como a los demás cursos y talleres ofertados por el Órgano Garante Local, deberá inscribirse y generar una cuenta en la plataforma CAVA INFO, ingresando a la liga siguiente:

<https://cava.infocdmx.org.mx/>

En esta misma liga se podrá consultar en el apartado de "Tutoriales", la guía para realizar de forma correcta la inscripción a dicha plataforma además del contenido de la plataforma, consultando los tutoriales denominados "¿Cómo registrarse a la plataforma CAVA INFO?" y "Un recorrido por la plataforma CAVA INFO"

Para complementar la capacitación en las materias antes señaladas, podrán realizar los diferentes cursos que ofrece el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ingresando a su plataforma de capacitación (CEVINAI), en la liga siguiente:

<https://cevifaipublica.inai.org.mx/>

En el caso de las personas servidoras públicas que sean integrantes del Comité de Transparencia, sus suplentes, así como a los enlaces de transparencia y protección de datos personales designados, además de los cursos antes citados, deberán de capacitarse en alguno de los Talleres especializados presenciales o en Aula Virtual en tiempo real como son: Taller de Solicitudes de Información y Recurso de Revisión, Taller de Clasificación de Información y Elaboración de Versiones Públicas y Taller Prueba de Daño, ofertados por el Órgano Garante Local, ingresando y registrándose en la plataforma CAVA INFO en la liga y conforme a las indicaciones referidas.

Handwritten signatures and initials in blue ink on the right margin of the page.



Para la obtención de la certificación 100% Capacitados de la Secretaría que emite el Órgano Garante Local, será necesario que todos los servidores públicos de estructura, se capaciten y se encuentren actualizados anualmente en los cursos que para tal efecto solicite el Órgano Garante Local.

Los titulares de las áreas operativas y administrativas deberán de implementar las acciones necesarias a efecto de que su personal de estructura cumpla con la capacitación y certificación correspondiente, debiendo remitir mediante oficio a la UT, las constancias que acrediten su capacitación, oficio mediante el cual se deberán adjuntar las constancias correspondientes de los cursos requeridos y el formato respectivo debidamente llenado.

13.2 De la Participación en la Promoción de la Cultura de la Transparencia, el Derecho de Acceso a la Información Pública y Rendición de Cuentas.

La UT será la encargada de comunicar a todas las áreas respecto de las convocatorias que emitan los Órganos Garantes para la participación de esta Secretaría en las actividades, mesas de trabajo, exposiciones, concursos, seminarios, diplomados, talleres, y toda actividad que fortalezca los derechos tutelados, siendo responsabilidad de los titulares de las áreas, la difusión al interior de su área así como incentivar la participación de las personas servidoras públicas.

[Handwritten notes and signatures in blue ink on the right margin]



14. DE LAS SANCIONES Y RESPONSABILIDADES.

Son causas de sanción por incumplimiento de las obligaciones establecidas en la **Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México**, las siguientes:

- I. La falta de respuesta a las solicitudes de información en los plazos señalados en la normatividad aplicable;
- II. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes en materia de acceso a la información o bien, al no difundir la información relativa a las obligaciones de transparencia previstas en la presente Ley;
- III. Incumplir con las obligaciones y los plazos de atención previstos en la presente Ley;
- IV. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, sin causa legítima, conforme a las facultades correspondientes, la información que se encuentre bajo la custodia de los sujetos obligados y de sus personas servidoras públicas o a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
- V. Entregar información incomprensible, incompleta, en un formato no accesible, una modalidad de envío o de entrega diferente a la solicitada previamente por el usuario en su solicitud de acceso a la información, al responder sin la debida motivación y fundamentación establecidas en esta Ley;
- VI. No actualizar la información correspondiente a las obligaciones de transparencia en los plazos previstos en la presente Ley;
- VII. Declarar con dolo o negligencia la inexistencia de información cuando el sujeto obligado deba generarla, derivado del ejercicio de sus atribuciones, facultades, competencias o funciones;
- VIII. Declarar la inexistencia de la información cuando exista total o parcialmente en sus archivos;
- IX. No documentar con dolo o negligencia, el ejercicio de sus facultades, competencias, funciones o actos de autoridad, de conformidad con la normatividad aplicable;
- X. Realizar actos para intimidar a los solicitantes de información o inhibir el ejercicio del derecho;
- XI. Denegar intencionalmente información que no se encuentre clasificada como reservada o confidencial;

[Handwritten signatures and initials in blue ink on the right margin]



- XII. Clasificar como reservada, con dolo o negligencia, la información sin que se cumplan las características señaladas en la presente Ley. La sanción procederá cuando exista una resolución previa del organismo garante, que haya quedado firme;
- XIII. No desclasificar la información como reservada cuando los motivos que le dieron origen ya no existan o haya fenecido el plazo, cuando el Instituto determine que existe una causa de interés público que persiste;
- XIV. No atender los requerimientos establecidos en la presente Ley, emitidos por Instituto, o
- XV. No acatar las resoluciones emitidas por el Instituto, en ejercicio de sus funciones.

El Instituto establecerá los criterios para calificar las sanciones conforme a la gravedad de la falta, en su caso, las condiciones económicas del infractor y la reincidencia. Asimismo, contemplará el tipo de sanciones, los procedimientos y plazos para su ejecución. Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

El Instituto, en el ámbito de sus competencias, podrá imponer, las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

- I. Amonestación pública, o
- II. Multa, de ciento cincuenta hasta mil quinientas veces la unidad de medida vigente en la Ciudad de México.

Son causas de sanción por incumplimiento de las obligaciones establecidas en la **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México** 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 presente Ley;

Handwritten signatures and initials in blue ink on the right margin.



- 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 establecido en la presente Ley;
- VII. No establecer las medidas de seguridad en los términos que establece la presente Ley;
- 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 presente Ley;
- 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 presente Ley;
- XII. No acatar las resoluciones emitidas por el Instituto; y
- XIII. Omitir la entrega del informe anual y demás informes o bien, entregarlo de manera extemporánea.

Las causas de responsabilidad previstas en las fracciones I, II, IV, IX, XI y XIII, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

En ambos casos las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

15. VALIDACIÓN Y APROBACIÓN DE LA ACTUALIZACIÓN DE LOS LINEAMIENTOS PARA LA OPERACIÓN DE LA UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO

CON FUNDAMENTO EN LO DISPUESTO EN EL ARTÍCULO 90 FRACCIÓNES I Y XIII Y 93 FRACCIÓN III DE LA LEY DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y RENDICIÓN DE CUENTAS DE LA CIUDAD DE MÉXICO Y ARTÍCULOS 75 FRACCIÓN II Y 76 FRACCIÓN V DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO, SE PROCEDE A LA VALIDACIÓN DE LA

[Handwritten signatures and initials in blue ink on the right margin]



ACTUALIZACIÓN DE LOS LINEAMIENTOS PARA LA OPERACIÓN DE LA UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO POR EL COMITÉ DE TRANSPARENCIA, EN SU DÉCIMA SEGUNDA SESIÓN EXTRAORDINARIA, CELEBRADA EL DÍA VEINTISÉIS DE ABRIL DE DOS MIL VEINTITRES.

PRESIDENTA

DIRECTORA EJECUTIVA DE LA UNIDAD DE TRANSPARENCIA
MTRA. NAYELI HERNÁNDEZ GÓMEZ

SECRETARIO TÉCNICO

SUBDIRECTOR DE TRANSPARENCIA
LIC. ISMAEL MAC DONALD ARGONZA

INTEGRANTE

DIRECTORA GENERAL DE ASUNTOS JURÍDICOS
COMISARIA MTRA.
MA. JACQUELINE FLORES BECERRA

INTEGRANTE

SUBSECRETARIO DE OPERACIÓN POLICIAL
COMISARIO JEFE
ISRAEL BENITEZ LÓPEZ

INTEGRANTE

TÍTULAR DEL ÓRGANO INTERNO DE CONTROL EN LA SECRETARÍA DE SEGURIDAD CIUDADANA
MTR. MARIO GARCÍA MONDRAGÓN

Handwritten signatures and initials in blue ink on the right margin.

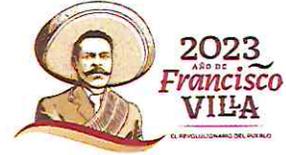


INTEGRANTE
[Firma manuscrita]
SUBSECRETARIO DE CONTROL DE TRÁNSITO
COMISARIO JEFE
FRANCISCO JAVIER MORENO MONTAÑO

INTEGRANTE
[Firma manuscrita]
SUBSECRETARIO DE PARTICIPACIÓN CIUDADANA Y PREVENCIÓN DEL DÉLITO
COMISARIO JEFE
LIC. PABLO VÁZQUEZ CAMACHO

INTEGRANTE
[Firma manuscrita]
SUBSECRETARIA DE DESARROLLO INSTITUCIONAL
COMISARIA JEFE
LIC. MARCELA FIGUEROA FRANCO

INTEGRANTE
[Firma manuscrita]
SUBSECRETARIO DE INTELIGENCIA E INVESTIGACIÓN POLICIAL
COMISARIO JEFE
DR. H.C. HERMENEGILDO LUGO LARA



INTEGRANTE

DIRECTOR GENERAL DE ASUNTOS INTERNOS
COMISARIO JEFE
LIC. RUBÉN ADRIAN DEHEZA ISLAS

INVITADO PERMANENTE

JEFE DE LA UNIDAD DEPARTAMENTAL DE IMPRESIONES Y DESARROLLO ARCHIVÍSTICO Y ENCARGADO DE LA UNIDAD COORDINADORA DE ARCHIVOS
MTRO. OMAR SANDOVAL BADILLO

INTEGRANTE

DIRECTORA EJECUTIVA DE COMUNICACIÓN SOCIAL
INSPECTORA GENERAL
MTRA. TANIA GUADALUPE AGUILAR DÍAZ

INTEGRANTE

OFICIAL MAYOR DE LA SECRETARÍA DE SEGURIDAD CIUDADANA
COMISARIO JEFE
LIC. CELSO SÁNCHEZ FUENTEVILLA

T

Handwritten notes and signatures on the right side of the page, including a large 'T' and several illegible signatures.



INTEGRANTE

SUBSECRETARIO DEL SISTEMA PENITENCIARIO
COMISARIO JEFE
LIC. OMAR REYES COLMENARES

INTEGRANTE

DIRECTOR GENERAL DE SEGURIDAD PRIVADA Y COLABORACIÓN INTERINSTITUCIONAL
LIC. IGNACIO MARMOLEJO LARIOS

[Handwritten signatures and initials in blue ink, including 'GT', 'M', 'X', 'e', 'd', 'sc', 'H']

LAS PRESENTES FIRMAS FORMAN PARTE INTEGRANTE DE LOS LINEAMIENTOS PARA LA OPERACIÓN DE LA UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO APROBADOS POR EL COMITÉ DE TRANSPARENCIA EN LA DÉCIMA SEGUNDA SESIÓN EXTRAORDINARIA, CELEBRADA EL DÍA VEINTISÉIS DE ABRIL DE DOS MIL VEINTITRES.