GOBERNACIÓN

SECRETARÍA DE GOBERNACIÓN

MANUAL DE PROCEDIMIENTOS PARA LA PROTECCIÓN Y ATENCIÓN DEL DERECHO DE ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y PORTABILIDAD DE DATOS PERSONALES DE LA SECRETARÍA DE GOBERNACIÓN Y SUJETOS OBLIGADOS COORDINADOS

UNIDAD DE TRANSPARENCIA DE LA SECRETARÍA DE GOBERNACIÓN

ÍNDICE

INTRODUCCIÓN

El derecho a la protección de los datos personales es un derecho humano relativamente nuevo en términos históricos, ya que su reconocimiento formal comenzó a tomar forma a finales del siglo XX y principios del XXI, coincidiendo con el auge de las tecnologías de la información y la digitalización.

Podemos localizar los antecedentes de la protección de datos personales con la Declaración Universal de los Derechos Humanos, la cual fue celebrada en 1948 en París, Francia, en la cual, dentro de su artículo 12 declara el derecho de preservar la privacidad de las personas [Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a la honra o a su reputación]; posteriormente, el convenio para la protección de los derechos humanos y las libertades fundamentales, así como el Pacto Internacional de Derechos Civiles y Políticos, refrendan el reconocimiento a la privacidad.[1]

La primera Ley sobre protección de datos personales se promulgó en Alemania Occidental en 1970, conocida como la Ley Federal de Protección de Datos (Bundesdatenschutzgesetz). Esta ley fue pionera en establecer normas para la recolección, almacenamiento y procesamiento de datos personales.

En 1981 se aprueba el primer instrumento vinculante en materia de datos personales, el Convenio 108 del Consejo de Europa.

En 1992, España aprobó la primera ley dedicada a la protección de datos personales, la Ley Orgánica 5/1992.

En 1995, la Unión Europea adoptó la Directiva de Protección de Datos (95/46/EC), que armonizó la legislación de protección de datos en los países miembros y estableció un marco sólido para proteger los datos personales de los europeos.

A partir del año 2000 y bajo el parámetro del Reglamento General de Protección de Datos, de la Unión Europea, en diversos países de América Latina desarrollaron sus propios instrumentos jurídicos de protección de datos personales, en el ámbito

[1] https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf

público como privado[2]; lo que ha servido como base para la creación de los instrumentos normativos en México.

En general, el derecho a la protección de los datos personales se ha convertido en un aspecto fundamental de los derechos humanos en la era digital, y su importancia sigue creciendo a medida que las tecnologías avanzan.

El fundamento jurídico para la protección de los datos personales se basa en una combinación de leyes nacionales e internacionales que establecen los derechos y las responsabilidades de los individuos y las organizaciones en relación con el manejo de datos personales.

Fundamento Jurídico Nacional

La Constitución Política de los Estados Unidos Mexicanos en el artículo 6 Apartado A, fracción II establece el derecho a la vida privada, derecho que comprende también la protección de datos personales.

En México dicha protección está regulada por la Ley de Datos, publicada en 2017. Esta establece las disposiciones y obligaciones para el manejo de datos personales por parte de los sujetos obligados (entidades públicas federales, estatales y municipales, incluyendo poderes ejecutivo, legislativo y judicial, así como órganos autónomos). Estos deben cumplir con los principios de protección de datos personales establecidos por la ley, incluyendo la licitud, finalidad, proporcionalidad, calidad, información, consentimiento y responsabilidad.

Fundamento Jurídico Internacional

- **Declaración Universal de los Derechos Humanos.** Adoptada por la Asamblea General de la ONU en 1948, establece el derecho a la privacidad en su artículo 12, lo cual ha sido una base para las leyes de protección de datos en todo el mundo.

- **Convenio 108 del Consejo de Europa.** El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), adoptado en 1981, fue uno de los

2 https://www.uasb.edu.ec/ciberderechos/2021/06/15/la-proteccion-de-datos-en-america-latina-influencia-del-rgpd/

primeros instrumentos internacionales vinculantes en esta área y ha sido un modelo para muchas leyes nacionales.

- **Reglamento General de Protección de Datos (GDPR).** Es una regulación de la Unión Europea implementada en 2018 que establece estándares rigurosos para la protección de datos personales y tiene un impacto global, ya que muchas organizaciones internacionales deben cumplir con sus disposiciones si manejan datos de ciudadanos europeos.

Derechos ARCOP

Son derechos que permiten a los individuos tener control sobre sus datos personales y cómo son tratados por las instituciones. ARCOP es un acrónimo que se refiere a los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad de datos personales.

Derecho de acceso: Se refiere al derecho de las personas a acceder a sus datos personales que están siendo procesados por una institución o entidad.

Derecho de rectificación: Este derecho permite a los individuos solicitar la corrección de cualquier información incorrecta o inexacta sobre ellos que esté siendo procesada por una institución.

Derecho de cancelación: Permite a quien lo solicita que sus datos personales sean eliminados por una organización cuando se cumplan ciertas condiciones.

Derecho de oposición: Es un derecho fundamental que permite a las personas oponerse al procesamiento de sus datos personales por parte de una institución.

Derecho de portabilidad: Permite solicitar que sus datos personales sean transferidos a ellos mismos o a otra entidad.

En definitiva, este manual busca resaltar la importancia de la protección de los datos personales como un elemento crucial para salvaguardar la privacidad, seguridad e integridad de los individuos, así como para mantener relaciones de confianza con las instituciones y garantizar el cumplimiento legal y ético en el manejo de la información personal dotando a las personas de las herramientas y recursos idóneos que les permitan tener control sobre su información.

OBJETIVO GENERAL

Establecer de manera sistematizada las bases para que cada Unidad Administrativa y Sujetos Obligados Coordinados de la Secretaría de Gobernación, realicen las gestiones necesarias a fin de cumplir con los principios, deberes y obligaciones, así como para que brinden la atención de las solicitudes de los titulares de los datos personales para dar cabal cumplimiento a lo estipulado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Lineamientos Generales de Protección de Datos Personales para el Sector Público y demás disposiciones de la materia, y así ser facilitadores del ejercicio de este derecho humano, de la protección de los datos personales y generar elementos que permitan construir sociedades pacíficas.

Este manual está enmarcado en el cumplimiento al Objetivo de Desarrollo Sostenible No. 16 "Paz, Justicia e Instituciones Sociales". Así como con sus líneas de acción No. 16.3; 16.5; 16.6 y 16.10[3].

[3] 16.3 Promover el estado de derecho en los planos nacional e internacional y garantizar la igualdad de acceso a la justicia para todos

16.5 Reducir considerablemente la corrupción y el soborno en todas sus formas

16.6 Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas

16.10 Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales

ÁMBITO DE APLICACIÓN

La aplicación y cumplimiento del presente instrumento es obligatorio para las personas Titulares de las Unidades Administrativas de la Secretaría de Gobernación responsables de cualquier tratamiento de datos personales con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, para establecer las medidas necesarias que garanticen la seguridad de los datos personales que en el ámbito de su competencia posean, recaben o transmitan, a fin de evitar su alteración, daño, destrucción o su uso, acceso o tratamiento no autorizado, pérdida y transmisión, debiendo asegurar su manejo para los propósitos para los cuales se hayan obtenido.

Para tales efectos se entenderán, además de las unidades administrativas previstas en el artículo 2 apartado B del Reglamento Interior de la Secretaría de Gobernación, como sujetos obligados coordinados, los siguientes:

- Comisión Nacional para Prevenir y Erradicar la Violencia Contra las Mujeres (**CONAVIM**);
- Coordinación para la Atención Integral de la Migración en la Frontera Sur (**CAIMFS**);
- Instituto Nacional para el Federalismo y el Desarrollo Municipal (**INAFED**);
- Secretaría Ejecutiva del Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes (**SIPINNA**);
- Fideicomiso para el cumplimiento de obligaciones en materia de los derechos humanos (**FCOMDH**);
- Fideicomiso para la plataforma de infraestructura, mantenimiento y equipamiento de seguridad pública y de aeronaves (**FIPIMESPA**);
- Fondo de apoyo social para ex trabajadores migratorios mexicanos (**EXBRACEROS/FONDEX**);

- Fondo para la protección de personas defensoras de derechos humanos y periodistas (**FPPDDHP**), y

- Comisión Nacional de Búsqueda de Personas (**CNBP**).

Por lo que hace a los órganos administrativos desconcentrados, Instituto Nacional de Migración; Secretaría General del Consejo Nacional de Población, y la Coordinación General de la Comisión Mexicana de Ayuda a Refugiados, no les serán aplicables el presente manual, en virtud de que estos podrán emitir, dentro de su ámbito de competencia, normativa en la materia, a través de sus Unidades de Transparencia.

FUNDAMENTO LEGAL

De manera enunciativa, más no limitativa, se enlistan las siguientes disposiciones legales que sustentan el ejercicio del derecho de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, así como su protección por parte de este sujeto obligado.

CONSTITUCIÓN

- Constitución Política de los Estados Unidos Mexicanos, y sus reformas.

LEYES

- Ley Orgánica de la Administración Pública Federal y sus reformas.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública y sus reformas.
- Ley Federal de Transparencia y Acceso a la Información Pública y sus reformas.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley General de Archivos y sus reformas.

REGLAMENTOS

- Reglamento Interior de la Secretaría de Gobernación.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

DOCUMENTOS NORMATIVO-ADMINISTRATIVOS

- Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública.
- Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.
- Lineamientos que establecen el procedimiento de denuncia por incumplimiento a las obligaciones de transparencia previstas en los artículos 70 a 83 de la Ley General de Transparencia y Acceso a la Información Pública y 69 a 76 de la Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos para determinar los catálogos y publicación de información de interés público; y para la emisión y evaluación de políticas de transparencia proactiva.
- Lineamientos generales para la organización y conservación de los archivos del Poder Ejecutivo Federal.
- Lineamientos que los sujetos obligados deben seguir al momento de generar información, en un lenguaje sencillo, con accesibilidad y traducción a lenguas indígenas.

OTRAS DISPOSICIONES

- Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.
- Políticas de Transparencia, Acceso a la Información Pública, Gobierno Abierto y Transparencia Proactiva de la Secretaría de Gobernación.
- Criterios de interpretación emitidos por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- Reglas de Operación para la Integración y Funcionamiento del Comité de Transparencia de la Secretaría de Gobernación y sus Sujetos Obligados Coordinados.
- Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno.
- Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hecho en Estrasburgo, Francia, el ocho de noviembre de dos mil uno.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta

al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

TÍTULO PRIMERO
DISPOSICIONES GENERALES

Capítulo I
Objeto del manual de procedimientos

Artículo 1.- El presente manual de procedimientos tiene por objeto sentar las bases que permitan realizar las gestiones necesarias para cumplir con las disposiciones en materia de protección y atención del derecho de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, las cuales son de observancia general para todas las áreas que integran la Secretaría de Gobernación y sus Sujetos Obligados Coordinados que realicen tratamiento de datos personales.

Artículo 2.- Para efectos del presente manual, se entenderá por:

I. **Acta(s):** Documento escrito que hace constar los acuerdos y decisiones tomadas en relación con lo acontecido durante la celebración de una sesión ordinaria o extraordinaria del Comité de Transparencia;

II. **Área(s) o Unidad(es) Administrativa(s):** Las mencionadas en el artículo 2 del Reglamento Interior de la Secretaría de Gobernación y su estructura organizacional, así como los sujetos obligados coordinados;

III. **Aviso de privacidad:** Documento que se pone a disposición de la persona titular de datos personales, de forma física, electrónica o en cualquier formato generado por la responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos; el cual puede ser integral o simplificado.

IV. **Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

V. **Bloqueo:** Consiste en la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles

responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

VI. **Comité:** Comité de Transparencia de la Secretaría de Gobernación y sus Sujetos Obligados Coordinados, cuya función es determinar la naturaleza de la información y que constituye el soporte fundamental para el entramado institucional que hace posible la transparencia, el acceso a la información pública, la protección de datos personales, la gestión archivística, la rendición de cuentas y la apertura institucional;

VII. **Consentimiento:** Manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

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

IX. **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, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

X. **Derechos ARCOP:** Los derechos de acceso, rectificación, cancelación, oposición y portabilidad de los datos personales;

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

XII. **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;

XIII. **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;

XIV. **Enlace(s) de Transparencia y en Datos Personales:** Las personas servidoras públicas designadas por los titulares de las áreas señaladas en el artículo 2 del Reglamento Interior de la Secretaría de Gobernación; y con las responsabilidades establecidas en el artículo 2, fracción V de las Políticas de Transparencia, Acceso a la Información Pública, Gobierno Abierto y Transparencia Proactiva de la Secretaría de Gobernación, a excepción de la Secretaría General del Consejo Nacional de Población; Coordinación General de la Comisión Mexicana de Ayuda a Refugiados y del Instituto Nacional de Migración;

XV. **Evaluación de Impacto en la Protección de Datos Personales:** Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, ponderan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;

XVI. **Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normativa aplicable;

XVII. **Información Clasificada:** Aquella que puede ser Reservada o Confidencial, de acuerdo con las causales establecidas en las disposiciones en la materia y que poseen las áreas señaladas en el artículo 2 del Reglamento Interior de la Secretaría de Gobernación, sus Órganos Administrativos Desconcentrados, o sus sujetos

obligados coordinados de acuerdo con sus facultades, competencias o funciones; a excepción de la Secretaría General del Consejo Nacional de Población; Coordinación General de la Comisión Mexicana de Ayuda a Refugiados y del Instituto Nacional de Migración;

XVIII. **Información Confidencial:** Aquella información cuya clasificación no estará sujeta a temporalidad alguna y se ubica en los supuestos señalados en los artículos 116 de la Ley General y 113 de la Ley Federal ambas de Transparencia y Acceso a la Información Pública; y que poseen las áreas señaladas en el artículo 2° del Reglamento Interior de la Secretaría de Gobernación, sus Órganos Administrativos Desconcentrados, o sus sujetos obligados coordinados de acuerdo con sus facultades, competencias o funciones; a excepción de la Secretaría General del Consejo Nacional de Población; Coordinación General de la Comisión Mexicana de Ayuda a Refugiados y del Instituto Nacional de Migración;

XIX. **Información Reservada:** Aquella información clasificada temporalmente, por ubicarse en alguno de los supuestos establecidos en los artículos 113 de la Ley General y 110 de la Ley Federal ambas de Transparencia y Acceso a la Información Pública; y que poseen las áreas señaladas en el artículo 2 del Reglamento Interior de la Secretaría de Gobernación, sus Órganos Administrativos Desconcentrados, o sus sujetos obligados coordinados de acuerdo con sus facultades, competencias o funciones; a excepción de la Secretaría General del Consejo Nacional de Población; Coordinación General de la Comisión Mexicana de Ayuda a Refugiados y del Instituto Nacional de Migración;

XX. **Instituto:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XXI. **Interés Jurídico:** Se entenderá por interés jurídico aquel derecho subjetivo derivado de una ley que permite a una persona actuar a nombre de otra que por su situación le es imposible. Ello, a efecto de solicitar el ejercicio efectivo de los derechos ARCO)

XXII. **Inventario de Datos Personales:** Catálogo de la información básica de cada tratamiento de datos personales, de conformidad con los artículos 33, fracción III de la Ley General de Protección de Datos

Personales y el 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público;

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

XXIV. **Ley Federal:** Ley Federal de Transparencia y Acceso a la Información Pública;

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

XXVI. **Lineamientos Generales:** Lineamientos Generales de Protección de Datos Personales para el Sector Público;

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

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

XXIX. **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;

XXX. **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 deben considerar las siguientes actividades:

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

XXXI. **OIC:** Órgano Interno de Control Especializado en el ramo Gobernación;

XXXII. **Orden del Día:** Determinación de todos aquellos puntos que sean relevantes y adecuados de tratar en el contexto de una sesión;

XXXIII. **Plan de Trabajo en materia de Política de Datos Personales:** Plan en el que se detalla el modo y conjunto de actividades a realizar para cumplir con las obligaciones y responsabilidades en materia de protección de datos personales, el cual incluye la elaboración de avisos de privacidad, análisis de brecha, análisis de riesgo y sistema de gestión de datos personales;

XXXIV. **Prueba de Daño:** Carga de los Sujetos Obligados de demostrar que la divulgación de la información lesiona el interés jurídicamente protegido por la Ley, y que el daño que puede producirse con la publicidad de la información es mayor que el interés de conocerla;

XXXV. **Programa de Protección de Datos Personales:** Documento programático que establece los elementos y las actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua;

XXXVI. **Políticas de Transparencia:** Políticas de Transparencia, Acceso a la Información Pública, Gobierno Abierto y Transparencia Proactiva de la Secretaría de Gobernación;

XXXVII. **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

XXXVIII. **Responsable(s):** Los sujetos obligados a que se refiere el artículo 1 de la Ley de Datos que deciden sobre el tratamiento de datos personales;

XXXIX. **RISEGOB:** Reglamento Interior de la Secretaría de Gobernación;

XL. **Secretaría:** Secretaría de Gobernación;

XLI. **Sesión Ordinaria:** Aquella que se desarrolla en la fecha establecida previamente por el Comité de Transparencia en su calendario anual de sesiones;

XLII. **Sistema de Gestión:** Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos

personales, de conformidad con lo previsto en la Ley de Datos y demás disposiciones que resulten aplicables a la materia;

XLIII. **Sujeto Obligado:** Cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos federales o realice actos de autoridad en los términos previstos en la Constitución Política de los Estados Unidos Mexicanos y la Ley General de Transparencia y Acceso a la Información Pública;

XLIV. **Sujetos Obligados Coordinados:** Sujetos obligados que no cuentan con el capital y la infraestructura necesaria para solventar las obligaciones de una Unidad de Transparencia, con excepción del Instituto Nacional de Migración; Secretaría General del Consejo Nacional de Población y la Coordinación General de la Comisión Mexicana de Ayuda a Refugiados;

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

XLVI. **Titular:** La persona física a quien corresponden los datos personales;

XLVII. **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la persona titular, responsable o encargada;

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

XLIX. **Unidad de Transparencia:** Unidad receptora de las solicitudes de información a cuya tutela estará el trámite de éstas.

Capítulo II
De la Unidad de Transparencia

Artículo 3.- La Unidad de Transparencia brindará asesoría a las Unidades Administrativas y en su caso, a los Sujetos Obligados Coordinados de la Secretaría en apego a los principios, deberes y obligaciones en materia de protección de datos personales establecidos en la Ley General, Ley Federal, Ley de Datos, el presente manual y demás disposiciones aplicables.

Artículo 4.- Además de lo dispuesto en los artículos 85 de la Ley de Datos, 45 de la Ley General y 61 de la Ley Federal, así como de lo estipulado en el artículo 6 de las Políticas de Transparencia, serán facultades de la Unidad de Transparencia:

I. Asesorar a las Unidades Administrativas y órganos administrativos desconcentrados de la Secretaría para la elaboración de programas de protección de datos personales, previo a la aprobación del Comité;
II. Realizar actividades de colaboración, coordinación, difusión y capacitación al interior de la Secretaría, directamente o con otros sujetos obligados, órganos garantes locales o federales u organizaciones de la sociedad civil, para fortalecer el conocimiento y pleno ejercicio del derecho constitucional de protección de datos personales;
III. Proponer al Comité las políticas, directrices, normas y criterios que sobre la materia resulte necesario implementar;
IV. Implementar al interior de la Secretaría mecanismos de comunicación, basados en la tecnología y el ahorro de recursos;
V. Dictaminar los Avisos de Privacidad, Programas de Gestión de datos, así como los documentos de seguridad que remitan las áreas, y
VI. Las demás que la persona Titular de la Secretaría y el Comité le confieran.

La persona Titular de la Unidad de Transparencia, será considerado como responsable únicamente para los tratamientos que correspondan a la referida unidad.

Capítulo III
Del Comité de Transparencia

Artículo 5.- El Comité es el órgano técnico, especializado, independiente e imparcial de la Secretaría de Gobernación, responsable de garantizar el ejercicio de los derechos de protección de datos personales, conforme a los principios y bases establecidos por el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos y demás disposiciones aplicables, cuya función es determinar la

naturaleza de la información en cumplimiento de las disposiciones en materia de transparencia, acceso a la información pública, protección de datos personales, gestión archivística, rendición de cuentas, así como para la apertura institucional.

El Comité, será la máxima autoridad al interior del sujeto obligado y velará por el debido cumplimiento y aplicación del presente manual.

Además de lo dispuesto en los artículos 84 de la Ley de Datos, 43 de la Ley General y 65 de la Ley Federal, así como de lo estipulado en las Políticas de Transparencia, y en las Reglas de Operación para la Integración y Funcionamiento del Comité de Transparencia de la Secretaría de Gobernación y sus Sujetos Obligados Coordinados, serán facultades del Comité de Transparencia:

I. Confirmar la clasificación de la información contenida en las versiones públicas que correspondan a la documentación solicitada y/o sus anexos —cuando sea el caso— propuestas por las áreas generadoras de la información, cuando ésta contenga datos personales, confidenciales y/o reservados, en términos de la legislación aplicable;
II. Cuando algún tema lo amerite, instruirá a la Secretaría Técnica, se tramite audiencia ante cualquier comisionado u autoridad del Instituto para ser atendido;
III. Determinar la viabilidad de retirar los asuntos del orden del día o se difiera para una sesión posterior, en los casos en que exista omisión o deficiencia en la entrega de la documentación relativa a las solicitudes de derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales;
IV. Aprobar los Avisos de Privacidad Integrales y Simplificados que emitan las Unidades Administrativas y los Sujetos Obligados Coordinados, tanto para tratamientos recurrentes, así como para tratamientos derivados de acciones concretas en el desarrollo de sus facultades y atribuciones, previa validación de la Unidad de Transparencia;
V. Proporcionar acompañamiento a las Unidades Administrativas y los Sujetos Obligados Coordinados que integren a los sujetos obligados y los coordinados, a través de la Unidad de Transparencia, en las auditorías que lleve el Instituto, en materia de datos personales, y
VI. Aprobar el plan de trabajo en materia de Política de Datos Personales.

Artículo 6.- El Comité de Transparencia podrá sugerir a las Unidades Administrativas y los Sujetos Obligados Coordinados de la Secretaría que realicen o dejen de hacer ciertas acciones con el fin de prevenir algún incumplimiento a las

disposiciones en materia de protección de datos personales.

Cuando adviertan un hecho que pueda constituir una probable falta administrativa en materia de datos personales en términos de la normativa aplicable, darán vista al OIC para su conocimiento.

Para los asuntos referentes a sus sesiones, funciones, organización, resoluciones y demás disposiciones del Comité de Transparencia, se estará a lo estipulado en las Reglas de Operación para la Integración y Funcionamiento del Comité de Transparencia de la Secretaría de Gobernación y sus Sujetos Obligados Coordinados[4].

Capítulo IV
De los Enlaces de Transparencia y de Datos Personales

Artículo 7.- Cada Unidad Administrativa y Sujeto Obligado Coordinado contará con un Enlace de Transparencia, quien será designado por su titular a través de oficio dirigido a la Unidad de Transparencia, dicho enlace será seleccionado de entre el personal adscrito a la Unidad Administrativa o Sujeto Obligado Coordinado de que se trate y tendrá un nivel mínimo de director de área u homólogo, o en su caso, justificar la designación realizada en favor de una persona con diverso nivel jerárquico.

Artículo 8.- Las personas Titulares de las Unidades Administrativas son las responsables del tratamiento de los datos personales en el ámbito de sus facultades y atribuciones; y, por lo tanto, tendrán la obligación de cumplir los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el presente manual y demás normativa aplicable.

Se precisa que no necesariamente, la figura de responsable deberá de recaer en la figura del Enlace de Transparencia.

Para los asuntos referentes a las atribuciones de los Enlaces de Transparencia, se estará a lo estipulado en las Políticas de Transparencia, Acceso a la Información

[4] Véase http://segob.gob.mx/es_mx/SEGOB/Acceso_a_la_informacion

Pública, Gobierno Abierto y Transparencia Proactiva de la Secretaría de Gobernación[5].

Capítulo V
Del Oficial de Protección de Datos Personales

Artículo 9.- El Oficial de Protección de Datos Personales, es la persona especialista en materia de protección de datos personales, quien tiene, entre otras atribuciones, la de auxiliar y orientar con relación al ejercicio del derecho a la protección de datos personales; asesorar a las áreas del sujeto obligado en materia de protección de datos personales; así como hacer las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales en posesión del responsable.

Artículo 10.- El Oficial de Protección de Datos Personales tendrá como atribuciones las siguientes:

I. Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales;
II. Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los Lineamientos generales;
III. Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los Lineamientos generales, previa autorización del Comité de Transparencia;
IV. Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales;
V. Trabajar con los equipos de tecnologías de la información (TI) y seguridad para auditar los sistemas de TI existentes e identificar dónde se almacenan los datos personales y cómo pueden verse comprometidos;
VI. Vigilar los programas de capacitación para garantizar que las personas servidoras públicas de las unidades administrativas y los Sujetos Obligados Coordinados comprendan los pormenores del cumplimiento de la Ley General;
VII. Evaluar las prácticas de recopilación y gestión de datos, así como

[5] Véase http://segob.gob.mx/es_mx/SEGOB/Acceso_a_la_informacion

recomendar procedimientos de capacitación, cumplimiento y documentar el proceso;

VIII. Recibir quejas de personas y autoridades, así como la atención y seguimiento de las mismas;

IX. Monitorear el cumplimiento, incluida la gestión de las actividades internas de protección de datos, asesorar sobre las evaluaciones de impacto de la protección de datos, capacitar a las personas servidoras públicas de las unidades administrativas y los Sujetos Obligados Coordinados y realizar auditorías internas;

X. Ser el primer punto de contacto para las consultas individuales y de otras autoridades en la materia;

XI. Desarrollar un mecanismo para evaluar la eficacia y eficiencia de estas políticas y/o prácticas;

XII. Ser el representante de la Secretaría en materia de protección de datos personales ante otros actores, sólo en caso de que la normatividad aplicable al sujeto obligado así lo disponga, y

XIII. Las demás que determine el responsable y la normatividad que resulte aplicable.

TÍTULO SEGUNDO
DE LOS PRINCIPIOS, OBLIGACIONES Y DEBERES

Capítulo I
De los Principios

Artículo 11.- Los principios de protección de datos personales son las herramientas para garantizar la efectiva protección de los datos personales cuando son tratados; las cuales son de uso obligatorio para interpretar y aplicar la Ley General y demás normativa aplicable, y representan un límite al tratamiento por parte del responsable.

Artículo 12.- Las personas servidoras públicas que traten datos personales directa o indirectamente, deberán en todo momento observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Artículo 13.- De la **Licitud**: El tratamiento de datos personales deberá sujetarse a las facultades y atribuciones legales del responsable, y en su caso, los aplicables del derecho internacional.

El sujeto obligado y los coordinados deberán identificar el marco normativo en el ámbito de sus atribuciones que se encuentre relacionado con el tratamiento de datos personales, el cual, deberá estar contemplado en el desarrollo del Sistema de gestión, aviso de privacidad integral y en el inventario de datos personales.

Los datos personales recabados no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Artículo 14.- De la **Finalidad**: El tratamiento deberá justificarse y determinarse conforme a los propósitos para los cuales se requieren los datos personales y deberán contar con las siguientes características:

I. **Concretas:** Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en la persona titular;
II. **Explícitas:** Cuando las finalidades se expresan y se dan a conocer de manera clara en el aviso de privacidad;
III. **Lícitas:** Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y
IV. **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento de su titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

Las finalidades serán del conocimiento de la persona titular de los datos personales a través del aviso de privacidad.

Se podrán dar finalidades distintas a las establecidas, siempre y cuando, el responsable esté legalmente facultado y se cuente con el consentimiento del titular; asimismo, se deberá considerar la expectativa razonable de privacidad del titular basada en la confianza que deposita cualquier persona en otra, respecto de sus datos personales serán tratados conforme a lo acordado; las consecuencias del tratamiento posterior de los datos personales para la persona titular, así como las

medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y los Lineamientos generales.

Asimismo, se proporcionará a las personas titulares los mecanismos para que puedan manifestar su negativa para las finalidades secundarias en su totalidad o parcialmente.

Artículo 15.- De la **Lealtad**: Se refiere a la obtención y tratamiento recto, privilegiando los intereses y expectativa de privacidad de las personas titulares, evitando los medios engañosos y fraudulentos, el dolo, mala fe o negligencia que den lugar a la discriminación, trato injusto o arbitrario de las personas titulares, por lo que se deberá verificar su estricto cumplimiento.

Artículo 16.- Del **Consentimiento**: Antes del tratamiento de datos personales, se deberá de contar con el consentimiento expreso o tácito previo de la persona titular, proporcionado de forma libre sin que medie error, mala fe, violencia o dolo específico relativo a las finalidades y de manera informada, a través del aviso de privacidad.

Será válido el consentimiento tácito siempre y cuando las disposiciones legales no exijan que la voluntad sea expresa y se entenderá otorgado cuando no exista manifestación negativa en contra; en caso de que no se recaben los datos directamente por el responsable, se tendrá un término de 5 días hábiles para obtenerlo, posteriores a que se ponga a disposición de la persona titular el aviso de privacidad.

Será expreso cuando obre de forma verbal, escrita o en medio electrónico, óptico o signos inequívocos a través de una declaración, acción afirmativa como la firma autógrafa, huella dactilar, firma electrónica o algún mecanismo equivalente autorizado por la normativa aplicable.

El consentimiento puede ser revocado en cualquier momento por la persona titular, sin que se le atribuyan efectos retroactivos, a través del ejercicio de cancelación y oposición.

No será necesario recabar el consentimiento de las personas titulares, conforme al artículo 22 de la Ley General, en los siguientes casos:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley General, en ningún caso, podrán contravenirla;
II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
IV. Para el reconocimiento o defensa de derechos de la persona titular ante autoridad competente;
V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y la persona responsable;
VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
VIII. Cuando los datos personales figuren en fuentes de acceso público;
IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o
X. Cuando la persona titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Al respecto, se deberán de implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que se requiera como la habilitación de casillas o espacios en el Aviso de Privacidad para expresar el consentimiento.

La actualización de alguna de las fracciones previas, no exime al responsable del cumplimiento de las demás obligaciones establecidas en la Ley de Datos y demás normativa aplicable.

Artículo 17.- De la **Calidad**: Se presume cumplida cuando la persona titular directamente proporciona sus datos personales y hasta que éste no manifieste y compruebe lo contrario; asimismo, se deberán adoptar las medidas necesarias para tener los datos:

I. **Exactos y completos**: Esto es que no presentan errores que pudieran afectar su veracidad;
II. **Correctos**: Su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable, y
III. **Actualizados**: Responden fielmente a la situación actual de la persona titular.

Se deberán establecer plazos de conservación y documentar los procedimientos para la conservación, bloqueo y supresión de los datos personales.

Artículo 18.- De la **Proporcionalidad**: Sólo deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios, es decir, no deben ser excesivos para el cumplimiento de las finalidades que motivaron su obtención y deben ir en concordancia con las atribuciones conferidas al responsable por la normatividad aplicable.

Se deberán realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, con relación a las finalidades; por lo que será necesario verificar que los datos personales recabados sean precisos a la finalidad, previo análisis y verificación.

Artículo 19.- De la **Información**: Informar a la persona titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto, con independencia de que no se requiera el consentimiento de la persona titular para el tratamiento de sus datos personales.

Se deberá elaborar y poner a disposición, a través de los medios que se consideren pertinentes, los avisos de privacidad simplificado e integral que correspondan al tratamiento que lleven a cabo, aun cuando no requiera el consentimiento de la persona titular.

Artículo 20.- De la **Responsabilidad**: Para cumplir con el principio de responsabilidad se adoptarán políticas y se implementarán mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones legales, como siguen:

I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
VI. Establecer procedimientos para recibir y responder dudas y quejas de las personas titulares;
VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley de Datos y las demás que resulten aplicables en la materia, y
VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley de Datos y las demás que resulten aplicables en la materia.

Adicionalmente, se deberá considerar el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance y finalidades del tratamiento de los datos personales; las atribuciones y facultades del responsable y demás cuestiones que considere convenientes, podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas, o cualquier otro mecanismo que determine adecuado.

Capítulo II
De los Deberes

Artículo 21.- Las Unidades Administrativas que integran la Secretaría de Gobernación y sus sujetos obligados coordinados que realicen tratamiento de datos personales, deberán cumplir con los deberes de seguridad y confidencialidad que las disposiciones normativas en la materia contemplan, los cuales prevén la protección de los datos personales de cualquier amenaza de riesgo con potencial para provocarles un daño o perjuicio.

Artículo 22.- Deber de **Seguridad**: Se deberán establecer y mantener las medidas de seguridad de carácter **administrativo, físico y técnico** para la protección de los datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, independientemente del sistema en el que se encuentren los datos personales y el tipo de tratamiento que efectúe.

Las medidas de seguridad antes señaladas constituyen mínimos exigibles, por lo que el responsable podrá adoptar las medidas adicionales que estime necesarias para brindar mayores garantías en la protección de los datos personales en su posesión.

Artículo 23.- Para la adopción de las medidas de seguridad, se deberá considerar:

I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Artículo 24.- Las medidas de seguridad **administrativas, físicas y técnicas**, estarán interrelacionadas con las siguientes actividades, las cuales deberán estar

documentadas y contenidas en un sistema de gestión, elaborados por las unidades administrativas y sujetos obligados coordinados que traten datos personales:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personas servidoras publicas responsables, entre otros;
V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y
VIII. Diseñar y aplicar diferentes niveles de capacitación de las personas servidoras públicas bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Artículo 25.- El Responsable deberá informar sin dilación alguna a la persona titular, y al Instituto, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el Responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que las personas titulares afectadas puedan tomar las medidas correspondientes para la defensa de sus derechos.

Artículo 26.- El responsable deberá informar a la persona titular al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones a la persona titular acerca de las medidas que ésta pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata;
V. Los medios donde puede obtener más información al respecto, y
VI. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

Artículo 27.- Deber de **Confidencialidad**: Los Responsables del tratamiento de datos personales deberán implementar mecanismos de control respecto de la obligación de secrecía de todas las personas servidoras públicas que intervengan dentro del proceso del tratamiento, aun cuando ya no participe en alguna fase del tratamiento.

En ese sentido, se impulsarán campañas de sensibilización para las personas servidoras públicas que participen en el tratamiento de datos, se verificará que los contratos y convenios contengan una cláusula de confidencialidad cuando exista transferencia o remisión de datos personales, así como todos los controles pertinentes para garantizar la confidencialidad de los datos personales que son tratados.

TÍTULO TERCERO
DE LA SEGURIDAD Y PROTECCIÓN DE LOS DATOS PERSONALES

Capítulo I
Del Documento de Seguridad

Artículo 28.- Conforme a las disposiciones legales, cada Unidad Administrativa y Sujeto Obligado Coordinado que trate datos personales, deberá realizar un documento de seguridad mediante el cual, de manera general, describa y de cuenta de las medidas de seguridad técnicas, físicas y administrativas implementadas para evitar el daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado de los datos personales, el cual será aprobado por el Comité de Transparencia.

Artículo 29.- El Documento de Seguridad deberá contener como mínimo, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El Plan de Trabajo en materia de Política de Datos Personales;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Artículo 30.- Acorde con lo dispuesto en la Ley General, el Documento de Seguridad se actualizará en los supuestos siguientes:

I. Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con el que se cuente;
III. Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida, y
IV. Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En dicha actualización participarán las personas titulares de las unidades administrativas y los sujetos obligados coordinados como responsables de los tratamientos, y previa solicitud, se someterán a discusión y análisis del Comité de Transparencia.

Capítulo II
De las Vulneraciones a la Seguridad de los Datos Personales

Artículo 31.- En términos de lo previsto en la Ley General y demás normativa aplicable, se consideran 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, y
IV. El daño, la alteración o modificación no autorizada.

Las personas Titulares de las Unidades Administrativas y los Sujetos Obligados Coordinados deberán llevar una bitácora de las vulneraciones a la seguridad en las que se describa la vulneración, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Artículo 32.- Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de las personas titulares de los datos personales, las personas Titulares de las Unidades Administrativas y los Sujetos Obligados Coordinados involucrados, deberán generar un informe detallado que contenga, al menos lo siguiente:

I. La hora y fecha de la identificación de la vulneración;
II. La hora y fecha del inicio de la investigación sobre la vulneración;
III. La naturaleza del incidente o vulneración ocurrida;
IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
V. Las categorías y número aproximado de personas titulares afectadas;
VI. Los sistemas de tratamiento y datos personales comprometidos;
VII. Las acciones correctivas realizadas de forma inmediata;
VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
IX. El medio puesto a disposición del o la titular para que pueda obtener mayor información sobre la vulneración y cómo proteger sus datos personales;
X. El nombre completo de la o las personas designadas para proporcionar mayor información al Instituto, en caso de requerirse, y
XI. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

La persona titular de la unidad administrativa que haya sufrido la vulneración, deberá remitir dentro de las 48 horas posteriores al incidente, el informe antes referido, para que la Unidad de Transparencia la haga del conocimiento del Comité de Transparencia y del Instituto en tiempo y forma.

Capítulo III
Del Programa de Protección de Datos Personales

Artículo 33.- El Programa de Protección de Datos Personales aportará el marco necesario para la protección de los datos personales en posesión de la Secretaría, promoverá la adopción de mejores prácticas en la materia, de manera preferente una vez que el programa se haya implementado de manera integral en la Secretaría, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos. Asimismo, fomentará el cumplimiento de los principios, deberes y obligaciones establecidos en la Ley General, en el presente manual y la normatividad que derive de los mismos.

Artículo 34.- La Unidad de Transparencia deberá de presentar al Comité de Transparencia el Programa de Protección de Datos Personales, para su aprobación el cual deberá contener:

I. Un diagnóstico sobre los problemas, las necesidades o áreas de oportunidad detectadas para el debido cumplimiento de los principios y deberes en materia de protección de datos personales dentro de la Secretaría;
II. Las actividades propuestas, su viabilidad, así como los objetivos que se persiguen, los cuales estarán vinculados a la atención de los problemas, las necesidades o áreas de oportunidad previamente detectadas, y
III. Los mecanismos de revisión de los cuales se velará su cumplimiento.

Capítulo IV
Del Programa de Capacitación y Actualización

Artículo 35.- La Secretaría y los Sujetos Obligados Coordinados contarán con un Programa de Capacitación y Actualización en materia de Protección de Datos Personales, como uno de los mecanismos a través de los cuales se cumplirá con el principio de responsabilidad, el cual considerará los niveles de capacitación atendiendo los roles y las responsabilidades de las personas servidoras públicas que realizan tratamiento de datos personales.

El Comité será el encargado de aprobar el Programa de Capacitación y Actualización en la materia, con base en la propuesta que sea presentada por la

Unidad de Transparencia, en la cual se consideren las necesidades de capacitación de las Unidades Administrativas.

TÍTULO CUARTO
DEL TRATAMIENTO REGULAR E INTENSIVO DE DATOS PERSONALES

Capítulo I
Del Aviso de Privacidad

Artículo 36.- Como parte de las acciones para cumplir con el principio de información, la Secretaría y los Sujetos Obligados Coordinados contarán con un aviso de privacidad integral y su correlativo aviso de privacidad simplificado, por cada tratamiento de datos personales, redactado en un lenguaje ciudadano, sencillo, claro y comprensible, considerando en todo momento el perfil de la persona titular al cual vaya dirigido, evitando el uso de:

I. Frases inexactas, ambiguas o vagas;
II. Incluir textos que induzcan a las personas titulares a elegir una opción en específico;
III. Marcar previamente casillas, en caso de que éstas se incluyan, para que las personas titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que las personas titulares han consentido el tratamiento de sus datos personales sin manifestación alguna de su parte, y
IV. Remitir a textos o documentos que no estén disponibles para las personas titulares.

En todo momento, las personas Titulares de las Unidades Administrativas, deberán asegurarse de que los Avisos de Privacidad se encuentren actualizados.

Artículo 37.- El Aviso de Privacidad cuenta con dos modalidades, el integral y el simplificado, el aviso integral, deberá estar permanentemente publicado en un lugar visible que facilite la consulta por parte de la persona titular y que le permita acreditar fehacientemente el cumplimiento de esta obligación ante el Instituto, ambos formatos pueden ponerse a disposición desde el primer momento.

Artículo 38.- El Aviso Integral contará con los elementos siguientes:

I. La denominación del responsable;

II. El domicilio del responsable;
III. Los datos personales que serán sometidos al tratamiento, identificando aquéllos que son sensibles;
IV. Las finalidades del tratamiento, distinguiendo aquellas que son necesarias de las que no lo son;
V. Las transferencias que se realicen, haciendo mención de los destinatarios y las finalidades;
VI. Los mecanismos y medios disponibles para que la persona titular pueda manifestar previamente su negativa para el tratamiento de sus datos personales;
VII. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
VIII. Los mecanismos, medios y procedimientos disponibles para ejercer los Derechos ARCO, y en su caso la portabilidad;
IX. El domicilio de la Unidad de Transparencia, y
X. Los medios a través de los cuales el responsable comunicará a las personas titulares los cambios al aviso de privacidad.

Artículo 39.- El Aviso Simplificado contará con los elementos siguientes:

I. La denominación del responsable;
II. Las finalidades del tratamiento, distinguiendo aquellas que son necesarias de las que no lo son;
III. Las transferencias de datos personales que requieran consentimiento, haciendo mención de las finalidades y los destinatarios.
IV. Los mecanismos y medios disponibles para que la persona titular pueda manifestar previamente su negativa para el tratamiento de sus datos personales.
V. El sitio donde se podrá consultar el Aviso de Privacidad Integral, y
VI. Fecha de elaboración o última actualización.

Artículo 40.- En aquellos casos en los que se suscite un cambio de denominación, cuando se requieran datos personales sensibles adicionales, se modifiquen las finalidades o las condiciones de transferencia o se prevea la realización de otras que requieran el consentimiento de la persona titular se deberá realizar un nuevo aviso de privacidad que prevea estas modificaciones.

Capítulo II
De las Medidas Compensatorias

Artículo 41.- De acuerdo con la Ley General, las medidas compensatorias son mecanismos alternos para dar a conocer a las personas titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance.

En tal consideración, las medidas compensatorias se actualizan cuando:

a) Existe imposibilidad de dar a conocer a la persona titular el aviso de privacidad de forma directa, y
b) Cuando le exija esfuerzos desproporcionados al responsable para dar a conocer a la persona titular el aviso de privacidad de forma directa.

Resulta importante señalar que, previo a instrumentar medidas compensatorias, el responsable debe cumplir con el principio de proporcionalidad el cual le establece la obligación de suprimir o eliminar todos aquellos datos personales que hayan dejado de ser necesarios para el cumplimiento de las finalidades que originaron su tratamiento.

Capítulo III
De la Evaluación de Impacto

Artículo 42.- La Evaluación de Impacto en la Protección de Datos Personales tiene por objeto:

I. Identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales;
II. Describir las acciones concretas para la gestión de los riesgos de los tratamientos intensivos o relevantes de datos personales;
III. Analizar y facilitar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables, respecto a tratamientos intensivos o relevantes de datos personales, y
IV. Fomentar una cultura de protección de datos personales al interior de la organización del responsable.

Artículo 43.- El responsable está en presencia de un tratamiento intensivo o relevante de datos personales, entre otros, cuando pretenda:

I. Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para las personas titulares;

II. Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de las personas titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de las personas titulares;

III. Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa mas no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica;

IV. Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos;

V. Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración de seguridad por la cantidad de información contenida en ellas, pudiera derivarse una afectación a la esfera personal de las personas titulares, sus derechos o libertades;

VI. Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas;

VII. Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala;

VIII. Permitir el acceso de terceros a una gran cantidad de datos personales que anteriormente no tenían acceso, ya sea, entregándolos, recibiéndolos y/o poniéndolos a su disposición en cualquier forma;

IX. Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia;

X. Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo a la persona titular;

XI. Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos;

XII. Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar;

XIII. Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales, o

XIV. La observación sistemática a gran escala de una zona de acceso público.

Artículo 44.- El responsable o responsables deberán elaborar y presentar ante la Unidad de Transparencia por si o en conjunto, una evaluación de impacto en la protección de datos personales. En caso de duda de su elaboración y obligación de presentarla, se podrá consultar a la Unidad de Transparencia, la cual, una vez que cumpla con los requisitos legales, la enviará al Instituto.

Artículo 45.- En la Evaluación de Impacto en la Protección de Datos Personales, el responsable deberá señalar, al menos, la descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar, la justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales; la representación del ciclo de vida de los datos personales a tratar; la identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales; el

análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con la Ley General y demás disposiciones aplicables; los resultados de la o las consultas externas que se efectúen; la opinión técnica del oficial de protección de datos personales, y cualquier otra información o documentos que considere conveniente hacer del conocimiento del Instituto o los organismos garantes en función de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar.

Artículo 46.- No será necesario realizar y presentar una Evaluación de Impacto en la Protección de Datos Personales cuando se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación o se trate de situaciones de emergencia o urgencia; para lo anterior, el responsable deberá presentar un informe en el domicilio del Instituto, durante los primeros treinta días posteriores a la fecha de la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, contados a partir del primer día de la puesta en operación o modificación de ésta, a través del cual, de manera fundada y motivada, señale:

I. La denominación y los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;
II. Las finalidades del tratamiento intensivo o relevante de datos personales;
III. Las razones o motivos que le permitieron determinar que la evaluación de impacto en la protección de datos personales compromete los efectos de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretende implementar o modificar, o bien, la situación de emergencia o urgencia que hacen inviable la presentación de ésta;
IV. Las consecuencias negativas que se derivarían de la elaboración y presentación de la evaluación de impacto en la protección de datos personales;

V. El fundamento legal que habilitó el tratamiento de datos personales en el marco de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que se pretende poner en operación o modificar;

VI. La fecha en que se puso en operación o modificó la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, así como su periodo de duración;

VII. La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso, y

VIII. Los mecanismos o procedimientos adoptados por el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con todas las obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables, así como todos los datos que resulten necesarios.

TÍTULO QUINTO
DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y PORTABILIDAD

Capítulo I
Del Ejercicio de los Derechos ARCOP de los Datos Personales

Artículo 47.- El derecho a la protección de datos personales es un derecho personalísimo, por lo que sólo la persona titular, o en su caso, el representante podrá solicitarlo, este derecho comprende el acceso, rectificación, cancelación, oposición y la portabilidad.

Artículo 48.- Para ejercer el derecho a la protección de datos personales, es necesario presentar una solicitud a través de los medios y mecanismos señalados por el responsable en el aviso de privacidad, asimismo, deberá contener el nombre de la persona titular, y en su caso el del representante, el medio para recibir notificaciones, señalar el derecho que quiere ejercer, la descripción clara y precisa del dato o datos al que desea acceder, rectificar (modificación solicitada), cancelar

(causas que la motivan), oponerse (situación que lleva a solicitar se finalice el tratamiento o alguna de las finalidades) o portar, y en su caso, los documentos que faciliten su localización.

Artículo 49.- En el caso de que la solicitud corresponda a la titularidad de personas menores de edad o fallecidas, además de los requisitos antes señalados, se deberá de presentar:

I. Acta de nacimiento de la persona menor de edad (o de quien corresponda la titularidad o en su caso, el acta de defunción);
II. Identificación oficial del padre, madre o quien ejerza el derecho;
III. En su caso una carta mediante la cual se manifieste, bajo protesta de decir verdad, que es la persona que ejerce la patria potestad y que no tiene limitado o suspendido ese ejercicio;
IV. Documento legal que acredite la tutela, en su caso;
V. Documento que acredite el interés jurídico;
VI. Así como una carta en la que se expresen los motivos por los cuales solicita el acceso, rectificación, cancelación, oposición o portabilidad.

Asimismo, deberá de acreditarse la identidad de la persona titular, y en su caso, el de la persona representante, a través de copia simple de una identificación oficial.

En el caso de personas menores de edad se podrá acreditar mediante acta de nacimiento y clave única del registro de población, credenciales de instituciones educativas o seguridad social.

Artículo 50.- Por lo que hace al representante legal de persona física, se acreditará con alguna de las siguientes tres opciones:

I. La presentación de una carta poder simple suscrita ante dos testigos, anexando copia simple de las identificaciones oficiales de los testigos;
II. Mediante instrumento público (documento suscrito por un Notario), o
III. Acudiendo la persona titular y su representante a declarar en comparecencia ante el responsable.

Para el caso de personas morales, únicamente se podrá acreditar mediante instrumento público.

Capítulo II
De los Plazos para la Atención

Artículo 51.- Dentro de los 20 días hábiles siguientes a la recepción de la solicitud, se deberá informar a la persona solicitante si procede o no el ejercicio del derecho solicitado. Si fuera procedente, deberá de realizar todas las gestiones necesarias para hacerlo efectivo.

De forma justificada, se podrá ampliar por un periodo igual, el plazo de atención bajo el procedimiento de ampliación del plazo de la Ley de Datos.

Artículo 52.- Si la solicitud no cuenta con los datos antes señalados, dentro del plazo de cinco días, se le prevendrá a fin de que subsane dentro de los diez días posteriores, en caso de no hacerlo, se tendrá por no presentada.

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

Artículo 53.- El ejercicio del derecho ARCOP es gratuito y sólo se podrá realizar el cobro por costos de reproducción, entregando de forma gratuita las primeras 20 fojas simples o certificadas a que haya lugar.

TRANSITORIOS

PRIMERO.- El presente manual entrará en vigor a partir de su aprobación por el Comité de Transparencia.

SEGUNDO.- El manual será notificado as a las personas Titulares de las Unidades Administrativas y Sujetos Obligados Coordinados de la Secretaría de Gobernación, asimismo, se publicará en el sitio de internet oficial.

TERCERO.- La Unidad de Transparencia elaborará y coordinará en conjunto con las Unidades Administrativas y Sujetos Obligados Coordinados de la Secretaría de Gobernación el Programa de Protección de Datos Personales, el cual deberá ser aprobado por el Comité de Transparencia.

GOBERNACIÓN

SECRETARÍA DE GOBERNACIÓN

HOJA DE FIRMA DEL MANUAL DE PROCEDIMIENTOS PARA LA PROTECCIÓN Y ATENCIÓN DEL DERECHO DE ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y PORTABILIDAD DE DATOS PERSONALES DE LA SECRETARÍA DE GOBERNACIÓN Y SUJETOS OBLIGADOS COORDINADOS

Dado en la Ciudad de México, a 22 de mayo de 2024.

SUPLENTE DEL PRESIDENTE DEL COMITÉ DE TRANSPARENCIA

DR. ALDO ANTONIO TRAPERO MALDONADO
COORDINADOR DE LEGISLACIÓN Y ESTUDIOS NORMATIVOS DE LA UNIDAD GENERAL DE ASUNTOS JURÍDICOS
SECRETARÍA DE GOBERNACIÓN