POLÍTICA INTERNA

PARA EL CUMPLIMIENTO DE PROTECCIÓN DE DATOS PERSONALES DE LA SECRETARÍA DE HONESTIDAD, TRANSPARENCIA Y FUNCIÓN PÚBLICA.

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES.

2025

Política Interna de Protección de Datos Personales

Contenido.

Página.

Política Interna de Protección de Datos Personales

1. Introducción.

El presente documento, se elaboró en cumplimiento de lo previsto en el artículo 24, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), normatividad que manifiesta la creación de políticas de protección de datos personales exigibles al interior del responsable de los datos, para dar cumplimiento al principio de responsabilidad establecido por la misma Ley.

En ese sentido, a efecto de salvaguardar el derecho humano a la protección de datos personales y en observancia al principio de responsabilidad que establece que el responsable del tratamiento de datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO se considera necesario emitir una política interna de protección de datos personales de observancia obligatoria para el personal de la Secretaría que realice un tratamiento de datos personales, la cual instituya un programa de trabajo dirigido a la protección de los datos personales en posesión del SHTFP.

Por ello, es responsable de proteger los datos personales que trate, garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, los deberes de seguridad y confidencialidad y las obligaciones derivadas de la Ley General.

El presente documento constituye una política interna de la SHTFP, elaborado en observancia al principio de responsabilidad, el cual prevé que quien es responsable del tratamiento de los datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en las disposiciones en materia de protección de datos personales.

Los responsables del tratamiento de los datos personales de la SHTFP, no sólo deben tomar las medidas necesarias para cumplir con los principios, deberes y obligaciones antes señaladas, sino que además es deseable que realice un esfuerzo adicional para observar las mejores prácticas y estándares en la protección de datos personales, buscando que en todo momento prevalezca la transparencia del uso y cuidado de la información personal que esté en su

posesión. Para ello, existe la autorregulación, mediante la cual, de manera voluntaria, los responsables pueden adoptar un mecanismo que les ayude a mejorar el tratamiento y cuidado de los datos personales.

Bajo esta tesitura, con la instrumentación de esta política de Protección de Datos Personales, se pretende facilitar a las personas Titulares de las Unidades Administrativas de esta Secretaría a realizar un tratamiento de datos personales en estricto apego a los principios, deberes y obligaciones establecidos en la Ley General y demás disposiciones aplicables, lo cual permitirá garantizar la adecuada protección de los datos personales y el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición y de Portabilidad a los datos personales "ARCOP" por parte de sus titulares.

2.- Objetivo.

Esta política tiene como objetivos los siguientes:

- ✓ Proporcionar los mecanismos, a través del cual el Oficial de Protección de Datos Personales de la Secretaría de Honestidad, Transparencia y Función Pública (SHTFP), asegurará la protección de los datos personales que estén en posesión de la Secretaría.
- ✓ Dar cumplimiento a las obligaciones en materia de protección de datos personales, establecidas en el artículo 19 de la Ley General de Protección de Datos Personales en posesión de sujetos Obligados.
- ✓ Promover una cultura de protección de datos personales mediante la implementación de buenas prácticas al interior de la Secretaría.
- ✓ Verificar el cumplimiento de las obligaciones y principios que establecen la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

3. Ámbito de aplicación.

La presente Política es de observancia general para todas las personas servidoras públicas adscritas a la SHTFP involucradas en el tratamiento de datos personales.

La aplicación y cumplimiento de la presente política, es obligatoria para las personas servidoras públicas Titulares de las Unidades Administrativas responsables de cualquier tratamiento de datos personales con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, así como establecer las medidas necesarias que garanticen la seguridad de los datos personales que 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. Lo anterior de conformidad con lo establecido en los artículos 3, fracción I y XXXI y 4 de la LGPDPPSO.

4. Marco Jurídico.

- Constitución Política de los Estados Unidos Mexicanos.
- Constitución Política del Estado Libre y Soberano del Estado de Oaxaca.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Oaxaca. (LPDPPSO).
- Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.

5. Glosario.

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

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Comité de Transparencia: Es un órgano colegiado, integrado por un número impar de servidores públicos que se formara de manera obligatoria al interior de cada sujeto obligado;

Datos personales: Cualquier información concerniente a una persona física identificada o identificable, que puede estar expresada en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, por ejemplo: nombre, apellidos, estado civil, domicilio, lugar y fecha de nacimiento, número telefónico, CURP, correo electrónico, grado de estudios, entre otros.

Es la información que nos describe, nos da identidad, nos caracteriza y diferencia de otros individuos.

Datos personales sensibles: Refieren información que pueda revelar aspectos íntimos de una persona, dar lugar a discriminación o su indebida utilización conlleva un riesgo grave, tal como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual.

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

Encargado del tratamiento de datos personales: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales por encargo del titular del banco de datos personales. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.

Enlace de datos personales: A las personas servidoras públicas designadas por las personas Titulares de las Unidades Administrativas de la SHTFP, a efecto de fungir como enlace ante el Comité de Transparencia y el Oficial de Datos Personales, en las responsabilidades que susciten en materia de protección de datos personales

Política Interna de Protección de Datos Personales

Inventario de datos personales: Identificación de las bases de datos de tratamiento de las Unidades Administrativas, por el cual, se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo cual se incluye el ciclo de vida del dato personal.

Oficial de Protección de datos Personales: Persona encargada de implementar, vigilar, controlar y promover la aplicación de la Política de Protección de Datos Personales al interior de la SHTFP.

Política: Política de tratamiento y gestión de datos personales, al referirnos en el presente documento a Política, se debe entender este documento en su totalidad.

Principios: El derecho a la protección de los datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones, estos son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que deciden sobre el tratamiento de datos personales.

SHTFP: Secretaría de Honestidad, Transparencia y Función Pública.

Titular: Persona física a quien corresponden los datos personales.

Tratamiento de datos personales: Conjunto de acciones de procesamiento de los datos personales (pueden ser: obtención, uso, divulgación o almacenamiento). El uso puede abarcar cualquier acción de acceso, manejo, aprovechamiento, transferencias o disposición de éstos.

CAPÍTULO I

Disposiciones Generales

Primera.- La presente Política es de observancia general para todo el personal de la SHTFP involucrado en el tratamiento de datos personales.

Segunda.- Corresponde al Comité de Transparencia, como máxima autoridad en materia de protección de datos personales, vigilar y verificar el cumplimiento de la presente Política de Protección de Datos Personales.

Tercera.- El Oficial de Protección de Datos Personales, asesorará a las Unidades Administrativas en materia de protección de datos personales, conforme a los principio, deberes y obligaciones establecidos en la LGPDPPSO, la presente Política y demás normatividad aplicable.

Cuarta.- Para las actividades señaladas en la presente Política, será necesario contar con personas servidoras públicas que funjan como enlaces en materia de datos personales en cada una de las unidades administrativas, las cuales serán designadas por la persona Titular de las mismas.

Quinta.- El Comité de Transparencia y/o el Oficial de Protección de Datos Personales podrán sugerir a las unidades administrativas que realicen o dejen de hacer diversas actividades a fin de cumplir con los principios, deberes y obligaciones en materia de protección de datos personales.

Sexta.- Las personas Titulares de las Unidades Administrativas son los responsables del tratamiento de los datos personales en el ámbito de sus funciones; y, por lo tanto, tendrán la obligación de cumplir los principios, deberes y obligaciones establecidos en la LGPDPPSO la presente Política y demás normativa aplicable.

Séptima.- El Comité de Transparencia y/o el Oficial de Protección de Datos Personales cuando adviertan un hecho que pueda constituir una presunta falta administrativa en materia de datos personales en términos de la normatividad aplicable, lo harán de conocimiento del Órgano Interno de Control, para los efectos conducentes.

CAPÍTULO II

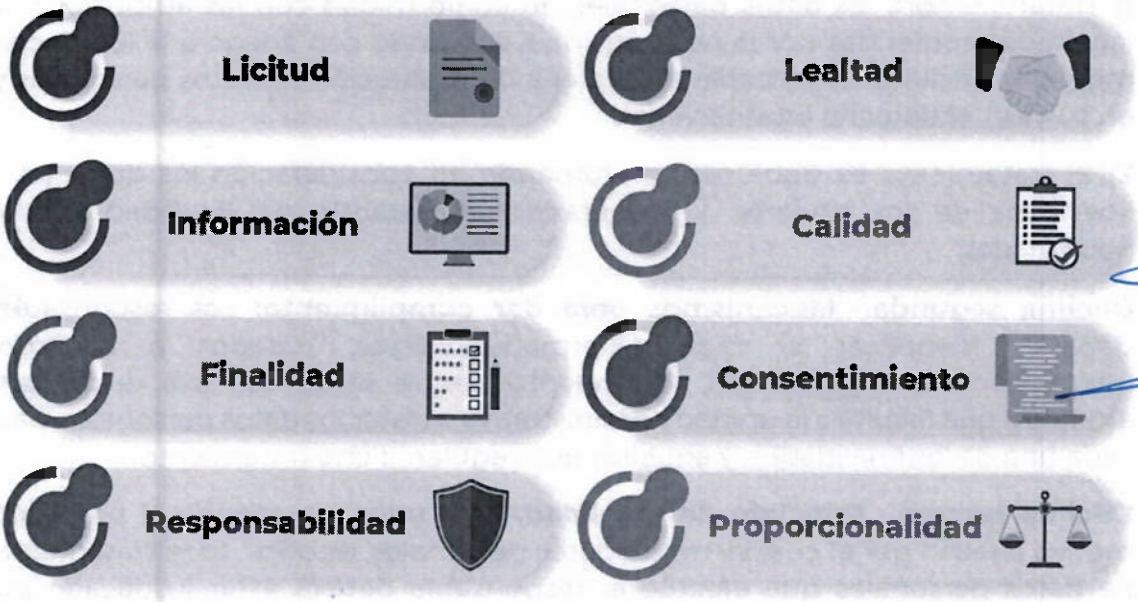
De los Principios de Protección de Datos Personales

Octava.- De conformidad con el artículo 16 de la LGPDPPSO los principios de protección de datos personales, son las herramientas muy valiosas para garantizar la efectiva protección de los derechos de los titulares de los datos personales frente al tratamiento de su información; herramientas de uso obligatorio para interpretar y aplicar la Ley General y demás normativa aplicable y representar un límite al tratamiento de datos personales que se encuentran en

posesión de sujetos obligados normativa aplicable y representar un límite al tratamiento de datos personales que se encuentran en posesión de sujetos obligados.

Novena.- El derecho a la protección de datos personales se rige a través de ocho principios, que son: Licitud, Finalidad, Lealtad, Consentimiento, Calidad, Proporcionalidad, Información y Responsabilidad.

Por lo tanto, las personas Titulares de las Unidades Administrativas de la SHTFP, para asegurar el correcto tratamiento de los datos personales deberán observar los principios rectores de la protección de datos personales.



Los principios son las reglas fundamentales de aplicación obligatoria para garantizar el respeto de las personas cuando sus datos recolectados, almacenados, usados o circulados han sido objeto de cualquier actividad por parte de responsables o encargados del tratamiento.

Estos principios tienen fuerza vinculante, aplicación práctica y son los que definen si un tratamiento de datos se está o no realizando de manera leal, lícita, transparente y adecuada.

Política Interna de Protección de Datos Personales

Para asegurar el correcto tratamiento de los datos personales en posesión de este Sujeto Obligado, la aplicación de estos principios se formaliza de la siguiente manera:

Décima.- Principio de Licitud. El tratamiento de datos personales por parte de las personas Titulares de las Unidades Administrativas de la SHTFP debe ser realizado de conformidad con las funciones y atribuciones o facultades que previamente se otorgan en la normativa aplicable que le confiera, en este sentido, no deben tratarse datos personales si no se sujetan a las facultades o atribuciones limitadas o definidas en la Ley.

Décima primera.- Obligaciones vinculadas al principio de licitud. Para cumplir el principio de licitud, el responsable tiene las siguientes obligaciones:

1) Tratar siempre los datos personales de conformidad con las atribuciones o facultades conferidas por la normatividad, actuando con apego a la legislación mexicana, incluida la aplicable en materia de protección de datos personales y, en su caso, el derecho internacional.

2) El tratamiento se debe realizar tomando en consideración los derechos y libertades de los titulares y respetando la garantía de legalidad de los gobernados.

Décima segunda.- Mecanismos para dar cumplimiento: Los responsables deberán Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales, para cada una de las finalidades, y aquellos que regulan dicho tratamiento.

Décima tercera.- Principio de Finalidad. Este principio atiende al propósito, motivo o razón por el cual se tratan datos personales, es decir, todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera, entendiéndose por estas lo siguiente:

✓ **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 el titular.

✓ **Explícitas:** Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.

✓ **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.

✓ **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 16 de la LGPDPPSO.

En ese sentido la finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

Ahora bien, en caso que los datos personales se traten para finalidades distintas a aquellas que motivaron su tratamiento original se deberán considerar 4 aspectos principales:

La expectativa razonable de privacidad del titular basada en la relación que tiene con éste.

- ✓ La naturaleza de los datos personales.
- ✓ Las consecuencias del tratamiento posterior de los datos personales para el titular.
- ✓ Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales.

En todo caso, el titular de los datos personales puede negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades distintas a aquellas que motivaron su tratamiento original, sin que ello tenga como consecuencia la conclusión del tratamiento para las finalidades originarias.

En ese sentido, es indispensable que en el aviso de privacidad se identifique y distinga las finalidades del tratamiento. Asimismo, se deberá indicar el mecanismo habilitado para que el titular, si así lo desea, pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades.

El responsable solo podrá realizar tratamiento para una finalidad distinta a las que fueron informadas previamente al titular en los siguientes supuestos:

- ✓ Se cuente con atribuciones legales y medie el consentimiento del titular, en términos de la LGPDPPSO.
- ✓ Una persona reportada como desaparecida.

Décima cuarta.- Obligaciones vinculadas al principio de finalidad. -Derivado del cumplimiento al principio de finalidad el responsable tiene las siguientes obligaciones:

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.

2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas.

3. Identificar y distinguir en el aviso de privacidad entre las finalidades que dan origen al tratamiento de aquellas que son distintas a las que lo originaron, pero se consideran compatibles y/o análogas.

4. Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias.

5. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como el correo postal, informar al titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información.

6. No condicionar el tratamiento para finalidades, con aquellas distintas a las que dieron origen al tratamiento.

7. Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento del titular de los datos.

Décima quinta.- Mecanismos para cumplir con el principio de finalidad.

1. Identificar las finalidades de cada tratamiento que se realice, y verificar que las mismas atiendan a fines específicos o determinados, y que sean acordes a las atribuciones o facultades del sujeto obligado y unidad administrativa de que se trate.

2. Verificar que en los avisos de privacidad se informan todas las finalidades para las cuales se tratan los datos personales, y que éstas se describen de manera clara.

3. Identificar qué finalidades requieren consentimiento y solicitarlo de acuerdo a lo establecido en la LGPDPPSO.

Décima séxta.- Principio de Lealtad. El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, para lo cual se deberá observar lo siguiente:

No se recaben datos personales con dolo, mala fe o negligencia.

No tratar los datos de tal manera que genere discriminación o un trato injusto contra los titulares.

No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado.

Se informen todas las finalidades del tratamiento en el aviso de privacidad. Con este principio no se permite el tratamiento, tramposo, deshonesto y no ético de la información sobre los titulares, los derechos del titular dependen del responsable, para que de esta manera el titular pueda confiar en la buena fe del responsable.

Décima séptima.- Obligaciones vinculadas al principio de lealtad. El responsable tiene las siguientes obligaciones en torno al principio de lealtad:

1) No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales.

2) Respetar en todo momento la expectativa razonable de privacidad del titular.

Décima octava.- Mecanismos para cumplir el principio de lealtad.

1) Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.

2) Verificar los tratamientos que realiza el sujeto obligado, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.

3) Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúa.

4) Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto.

5) Llevar a cabo el tratamiento de los datos personales sólo para los fines informados en el aviso de privacidad.

Décima novena.- Principio de Consentimiento. Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 16 de la LGPDPPSO, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

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

✓ **Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento.

✓ **Informada:** Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la LGPDPPSO, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

El consentimiento podrá manifestarse de las siguientes maneras:

✓ **Expreso.** Cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

✓ **Tácito**. Cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación

que al efecto se establezca, salvo en los casos previstos en el artículo 16 de la LGPDPPSO.

La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas.

De conformidad con el artículo 16 de la Ley General el consentimiento no se deberá recabar en los siguientes casos:

✓ Cuando una ley así lo disponga, debiendo ser acorde a las bases, principios y disposiciones establecidos en la normatividad en materia de datos personales.

✓ Cuando las transferencias se realicen entre responsables, se trate de datos personales que utilicen en el ejercicio de las facultades del sujeto obligado o sean compatibles o análogas con la finalidad que dio origen al tratamiento de los datos personales.

✓ Cuando exista una orden judicial, resolución o mandato fundado y motivado de una autoridad competente.

✓ Para el reconocimiento o defensa de derechos del titular ante autoridad competente.

✓ Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.

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

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

✓ Cuando los datos personales figuren en fuentes de acceso público.

✓ Cuando los datos personales se sometan a un procedimiento previo de disociación.

✓ Cuando el titular de los datos sea una persona reportada como desaparecida.

Sin embargo, aunque en dichos supuestos no se requiera el consentimiento para el tratamiento, se deberán cumplir los otros principios, lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.

El consentimiento expreso o por escrito se puede obtener a través del aviso de privacidad o de cualquier otro documento físico o electrónico que determine el responsable.

En caso que el responsable decidiera tratar los datos personales para finalidades distintas a las que informó originalmente en el aviso de privacidad, y para las cuales obtuvo el consentimiento inicial por parte de los titulares, será necesario solicitar el consentimiento de los titulares para las nuevas finalidades, siempre y cuando estas finalidades no actualicen los supuestos de excepción que señala el artículo 10 de la Ley General.

Vigésima.- Obligaciones vinculadas al principio de consentimiento. El responsable tiene las siguientes obligaciones en torno al principio de consentimiento.

1. Obtener el consentimiento del titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos previstos en el artículo 10 de la Ley General.

2. Solicitar el consentimiento siempre ligado a finalidades específicas e informadas en el aviso de privacidad.

3. Determinar el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito.

4. Solicitar el consentimiento expreso y por escrito para los datos personales sensibles, en caso de que no se actualice alguno de los supuestos del artículo 22 de la Ley General.

5. Solicitar el consentimiento expreso o por escrito cuando así lo requiera una ley o reglamento, se acuerde con el titular o lo determine conveniente el responsable.

6. Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento.

7. Solicitar el consentimiento previo a la obtención de los datos personales, si éstos se recaban directamente del titular y no se actualiza alguno de los supuestos previstos en el artículo 16 de la Ley General.

8. Solicitar el consentimiento antes de utilizar los datos personales para las finalidades para las cuales se obtuvieron, si éstos se recabaron de manera indirecta y no se actualiza alguno de los supuestos previstos en el artículo 16 de la Ley General.

9. Implementar medios sencillos y gratuitos para la obtención del consentimiento, de acuerdo con el tipo de consentimiento que se requiera (tácito, expreso o expreso y por escrito).

10. Llevar un control para identificar a los titulares que negaron su consentimiento y a las finalidades concretas para las cuales no se podrán tratar los datos personales.

11. Documentar su actuar para acreditar que se cumplió con el principio de consentimiento.

12. Solicitar el consentimiento si hubo cambios en las finalidades informadas en el aviso de privacidad y éstas lo requieren por no actualizarse alguno de los supuestos previstos en el artículo 16 de la Ley General.

Vigésima primera.- Mecanismos para cumplir con el principio de consentimiento.

1) En el caso del consentimiento expreso y por escrito, en todos los casos, deberá conservar el documento, físico o electrónico, que permita acreditar que obtuvo el consentimiento por parte del titular.

2) En el caso del consentimiento tácito, en virtud de que no hay una manifestación expresa del titular, las pruebas podrán ser aquéllas que permitan demostrar que el responsable puso a disposición de los titulares el aviso de privacidad.

3) Consentimiento expreso otorgado por los titulares y la solicitud respectiva.

4) Aviso de privacidad y procedimiento para su puesta a disposición.

5) Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.

6) Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.

7) Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.

8) Habilitar los mecanismos necesarios para solicitar el consentimiento expreso, en los términos señalados en la columna anterior, así como documentar su obtención.

9) Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.

10) Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante.

11) Cuando los datos personales no los proporcione personal o directamente el titular o su representante, se deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado.

Vigésima segunda: Principio de Calidad.- El responsable deberá adoptar las medidas necesarias para tratar los datos personales para la finalidad o finalidades que fueron recabados, asimismo, a efecto de mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

En relación a lo anterior, se debe entender que los datos cumplen con dichas características cuando:

✓ **Exactos y correctos:** cuando en posesión del responsable no presentan errores que pudieran afectar su veracidad.

✓ **Completos**: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.

✓ **Actualizados**: cuando los datos personales responden fielmente a la situación actual del titular.

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

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

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, ni aquél que se requiera para cumplir con:

✓ Las disposiciones legales establecidas en la Ley General de Archivos.

✓ Las disposiciones aplicables en la materia de que se trate.

✓ Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

✓ El periodo de bloqueo.

El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de conformidad con el artículo 18 de la Ley General, asimismo, se deberá incluir mecanismos que permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, el responsable debe proceder a la supresión de los datos personales.

Por su parte, respecto de los datos personales sensibles, se deberá prever que se limite el periodo de tratamiento al mínimo indispensable.

Vigésima tercera.- Obligaciones vinculadas al principio de calidad. El responsable tiene las siguientes obligaciones en torno al principio de calidad:

1) Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

2) Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo.

3) Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.

4) Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley General de Archivos.

5) Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

6) En caso de que se requiera, demostrar que los datos personales se conservan, bloquean y suprimen cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación.

7) Implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completen, en las distintas bases de datos que estén a cargo de la unidad administrativa.

Vigésima cuarta.- Mecanismos para cumplir con el principio de calidad.

1) Base de datos actualizada y correcta.

2) Constancias o anotaciones sobre la rectificación realizada, en aquellos casos en que la misma haya sido procedente.

3) Instrumentos de clasificación archivística.

4) Documentación y evidencia que se genere con la implementación de los procedimientos para la conservación, bloqueo y supresión de los datos personales.

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

El principio de proporcionalidad establece la obligación del responsable de tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

De igual forma, el responsable deberá prever que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron, las cuales, deben ser acordes con las atribuciones conferidas al responsable y señaladas en el aviso de privacidad.

Vigésima séxta.- Obligaciones vinculadas al principio de proporcionalidad. En síntesis, de acuerdo con lo antes expuesto, el responsable tiene las siguientes obligaciones en torno al principio de proporcionalidad:

1) Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.

2) Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

3) Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.

4) Crear bases de datos con datos personales sensibles sólo cuando se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 16 de la Ley General en la materia.

Vigésima séptima.- Mecanismos para cumplir con el principio de proporcionalidad.

1) Avisos de privacidad.

2) Documentos, expedientes, archivos o bases de datos correspondientes al tratamiento.

3) Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.

Vigésima octava.- Información: El responsable deberá informar al 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 y puedan ejercer su derecho a la protección de su información personal.

En ese sentido, todo responsable que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad, por lo que se deberán tener el número de avisos de privacidad que resulten necesarios de acuerdo con los tipos de tratamientos que realicen.

La disposición del aviso de privacidad implica publicar en un lugar visible, accesible y gratuito, en el cual el titular, de manera informada, cuente con la posibilidad de conocer el tratamiento que se les dará a sus datos personales. En ese sentido, el responsable no está obligado a entregar una copia del aviso de privacidad al titular, al menos que éste lo solicite.

Vigésima novena.- Obligaciones vinculadas al principio de información. El responsable tiene las siguientes obligaciones en torno al principio de información:

1. Poner a disposición de los titulares el aviso de privacidad en los términos que fije la Ley General en la materia y sus Lineamientos, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales.

2. Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera personal y directa del titular.

3. Poner a disposición del titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público.

4. Poner a disposición del titular el aviso de privacidad previo a iniciar tratamiento de los datos personales para la finalidad para la que se obtuvieron (aprovechamiento), cuando éstos no se hayan obtenido de manera directa del titular, el tratamiento no requiera del contacto con él y se cuente con datos para contactarlo.

5. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades, cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.

6. Redactar el aviso de privacidad de manera que sea claro, comprensible, con una estructura y diseño que facilite su entendimiento, para su elaboración tomar en cuenta el perfil de los titulares y atender lo siguiente: no usar frases inexactas, ambiguas o vagas; no incluir textos o formatos que induzcan al titular a elegir una opción en específico; no premarcar casillas en las que se solicite el consentimiento del titular, y no remitir a textos o documentos que no estén disponibles.

7. Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.

8. Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales.

9. Demostrar el cumplimiento del principio de información, en caso de que así se requiera.

10. Cuando se utilice la modalidad integral del aviso de privacidad, incluir todos los elementos informativos previstos de la normatividad aplicable.

11. Cuando se utilice la modalidad simplificado del aviso de privacidad, incluir todos los elementos informativos correspondientes.

12. Elaborar y tener disponible para su consulta el aviso de privacidad integral, con independencia de que se ponga a disposición de los titulares el aviso de privacidad en su versión simplificada previo a la obtención o aprovechamiento de los datos personales.

13. No establecer cobros para la consulta del aviso de privacidad.

14. Cuando así ocurra, informar en su portal de Internet, a través de una comunicación o advertencia colocada en un lugar visible y a la cual se pueda acceder desde el momento en que se ingresa a dicho portal, que están siendo utilizadas tecnologías de rastreo, que a través de éstas se pueden recabar datos personales y la forma en cómo se pueden deshabilitar.

15. Poner a disposición de los titulares un nuevo aviso de privacidad en los siguientes casos:

✓ Cambie la identidad del responsable.

✓ Se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular.

✓ Se requiera tratarlos datos personales para nuevas finalidades que requieran el consentimiento del titular.

✓ Se requiera realizar nuevas transferencias que requieran el consentimiento del titular.

Trigésima.- Mecanismos para cumplir con el principio de información.

1) Aviso de privacidad.

2) Evidencia de la difusión del aviso de privacidad por el medio de comunicación masiva.

3) Procedimiento o medio para la puesta a disposición de los avisos de privacidad.

4) Lugares y medios en los que se difundieron y colocaron los avisos de privacidad.

5) Medios en que se encuentren los avisos de privacidad integrales.

Trigésima primera.- Responsabilidad. El responsable deberá adoptar políticas e implementar mecanismos para asegurar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales. Asimismo, para cumplir con este principio los responsables deberán rendir cuentas sobre el tratamiento y protección de datos personales a las personas titulares y a los organismos garantes.

Bajo este principio, los responsables del tratamiento están obligados a velar por la protección de los datos personales aun y cuando los datos estén siendo tratados por encargados. Asimismo, este principio supone que el responsable tome las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica, así como al momento de realizar transferencias nacionales o internacionales de datos personales.

Asimismo, para cumplir con dicho principio el responsable, deberá implementar los mecanismos previstos en el artículo 24 de la LGPDPPSO para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

Trigésima segunda.- Obligaciones vinculadas al principio de responsabilidad:

1) Prever presupuesto para la instrumentación de programas y políticas de protección de datos personales.

2) Elaborar un programa de protección de datos personales que contemple el cumplimiento obligatorio al interior de la organización del responsable.

3) Elaborar y aplicar un programa de capacitación y actualización de los servidores públicos en materia de protección de datos personales, de conformidad con el apartado de Capacitación de este Programa.

4) Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad, que prevea una revisión cada dos años o antes si es necesario por un cambio sustancial en el tratamiento.

5) Establecer un procedimiento para atender dudas y quejas de los titulares con las características señaladas en la columna anterior.

6) Diseñar o modificar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de forma tal que prevean la privacidad por diseño y por defecto descritas en la columna anterior.

7) En todos los casos generar pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.

8) Velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, aún por aquéllos comunicados a encargados;

9) Adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad, y

10) Tomar medidas para que los terceros con quienes mantiene una relación jurídica que implique el tratamiento de los datos personales, respeten el aviso de privacidad en el que se establezcan las condiciones de dicho tratamiento.

Trigésima tercera.- Mecanismos para acreditar el cumplimiento del principio de responsabilidad. Se debe tomar en cuenta que los mecanismos que adopte el responsable, además de garantizar el debido tratamiento, deben privilegiar los intereses del titular y su expectativa razonable de privacidad.

1) Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales, lo cual se deberá contemplar en el Presupuesto del ejercicio en curso, en la medida que las condiciones presupuestarias lo permitan.

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

3) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

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

5) 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.

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

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

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

Es importante señalar que los mecanismos señalados en la normatividad no son los únicos que podría adoptar el responsable para cumplir con el principio de responsabilidad. Puede optar por medidas adicionales o distintas que contribuyan a elevar los estándares de protección de datos personales y cumplir con la normativa que regula este derecho.

Capítulo III

De los deberes para la protección de datos personales

La Ley General y la LPDPSPEO establecen los deberes que observarán los responsables en el tratamiento de los datos personales los cuales se relacionan entre sí y tendrán como objetivo principal garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Trigésima cuarta.- Deber de confidencialidad. Para el cumplimiento de este deber los responsables deberán establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del

tratamiento de los datos personales, guarden confidencialidad respecto a éstos, aún después de concluir su relación con el responsable.

En los casos en los que el responsable cuente con un Encargado, deberá formalizar la relación respectiva mediante contrato o cualquier otro documento, en cual se establecerá como cláusula general relacionada con los servicios que este preste, el guardar confidencialidad respecto de los datos personales tratados.

En las actividades de tratamiento de datos personales, realizadas por el encargado, este no ostentará poder alguno de decisión sobre el alcance y contenido, de igual forma limitará sus actuaciones a los términos fijados por el responsable.

El responsable será corresponsable por las vulneraciones de seguridad ocurridas en el tratamiento de datos personales que efectué el encargado a nombre y por cuenta de este.

La relación entre el responsable y el encargado deberá formalizarse mediante contrato o cualquier otro instrumento jurídico que decida el responsable y que permita acreditar su existencia, alcance y contenido. El instrumento jurídico mediante el cual decida el responsable formalizar la relación de servicios que preste el encargado, deberá prever, al menos las siguientes cláusulas generales:

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

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

✓ Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

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

✓ Guardar confidencialidad respecto de los datos personales tratados;

✓ Suprimir y 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, y

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

Para la prestación de los servicios del encargado, además de las cláusulas generales anteriores, el responsable deberá prever en el instrumento jurídico las siguientes obligaciones:

✓ Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales.

✓ Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y demás normatividad aplicable en la materia, proporcionando información y documentación que se estime necesaria para tal efecto, y

✓ Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la Ley General, las disposiciones aplicables, así como lo establecido en el aviso de privacidad que corresponda.

Al momento de realizar transferencias de datos personales nacionales o internaciones, el responsable deberá aplicar el principio de responsabilidad.

El encargado también podrá subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie autorización expresa de este último, como consecuencia el subcontratado asumirá el carácter de encargado conforme a lo establecido en la Ley General y demás disposiciones que resulten aplicables en la materia.

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

Obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de algún instrumento jurídico que decida, el cual permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en la Ley General.

Para los servicios de subcontratación que impliquen tratamiento de datos personales, el instrumento jurídico que suscriba el encargado con el subcontratado deberá prever, al menos las cláusulas generales y las obligaciones antes descritas.

Asimismo, para el caso en que existan tratamientos de datos personales en los que el responsable se adhiera a servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, mediante condiciones o cláusulas generales de contratación; exclusivamente podrá utilizar servicios en los que el o los proveedores guarden confidencialidad respecto de los datos personales sobre los que se preste el servicio.

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

Los proveedores de servicios de cómputo en la nube y otras materias que impliquen tratamiento de datos personales, para efectos de la Ley General y demás disposiciones aplicables en la materia, tendrán el carácter de encargados.

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

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:

✓ Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley General y demás normatividad aplicable en la materia;

✓ Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;

✓ Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y

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

Cuente con mecanismos, al menos, para:

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

✓ Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

✓ Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;

✓ Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, e

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

El responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.

Para el caso que el encargado y subcontratado incumplan las obligaciones contraídas con el responsable y decidan y determinen por si mismos, los fines, medios y demás cuestiones relacionadas con el tratamiento de los datos personales, asumirán el carácter de responsable de conformidad con la normatividad que les resulte aplicable en función de su naturaleza pública o privada.

Por otra parte, cuando el responsable realice algún tipo de transferencia, el receptor de los datos personales deberá llevar a cabo el tratamiento de datos personales, garantizando su confidencialidad.

Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular. Por regla general, el consentimiento será tácito, salvo que una ley exija al responsable recabar el consentimiento expreso del titular para la transferencia de sus datos personales.

Política Interna de Protección de Datos Personales

La Ley General, establece excepciones a las transferencias de datos, en las cuales el responsable no estará obligado a recabar el consentimiento del titular.

Todas las transferencias deberán formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, conforme a la normatividad aplicable al responsable, las cuales permitirán demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes, limitando el tratamiento de los datos personales transferidos a las finalidades que la justifiquen.

Al momento de realizar transferencias de datos personales nacionales o internaciones, el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General y demás disposiciones aplicables en la materia.

Los casos de excepción se dan cuando:

✓ Tratándose de una transferencia nacional y se realice entre responsables, en el cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos;

✓ Tratándose de una transferencia internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México,

✓ La transferencia internacional, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y el responsable receptor sean homólogas, o

✓ Las finalidades que motivan la transferencia internacional sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

Tanto en las transferencias nacionales como en las internacionales, el responsable, deberá comunicar al receptor de los datos personales el aviso de privacidad, mediante el cual se tratan los datos personales del titular.

Tratándose de transferencias nacionales, el receptor de los datos personales asume el carácter de responsable, y deberá tratar los datos personales comprometiéndose a garantizar la confidencialidad y únicamente los utilizará

para los fines que fueron transferidos, atendiendo a lo contenido en el aviso de privacidad que le será comunicado por el responsable transferente.

Para el caso de transferencias fuera del territorio nacional, el responsable sólo podrá realizarlas cuando el tercero receptor, encargado o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las establecidas en la Ley General y demás normatividad aplicable en la materia, así como los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente.

Trigésima sexta.- Obligaciones vinculadas al deber de confidencialidad.

1) Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

2) Incluir en las medidas de seguridad, controles para garantizar la confidencialidad de los datos personales.

3) Implementar los controles para la confidencialidad de los datos personales, sin perjuicio de lo establecido por la Ley General de Transparencia y Acceso a Información Pública.

4) Establecer cláusulas en los contratos con los encargados, que obliguen a la confidencialidad de los datos personales.

5) Implementar capacitación para los servidores públicos del Instituto, a fin de generar conciencia sobre la importancia de guardar la confidencialidad de los datos personales que tratan.

Trigésima sexta.- Mecanismos para acreditar el deber de confidencialidad.

1) Documento de seguridad.

2) Controles definidos para la confidencialidad de los datos personales.

3) Evidencia de la aplicación de los controles.

4) Contratos celebrados con los encargados del tratamiento.

5) Documentación que acredite la capacitación de los servidores públicos.

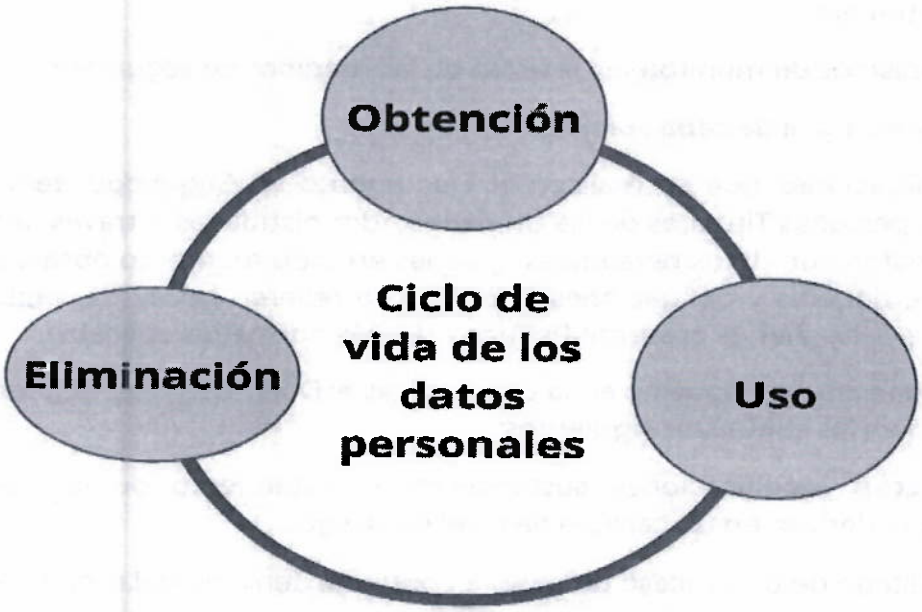
Capítulo IV

Documentos para la protección de los datos personales.

Para cumplir con dicho deber el responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales en su posesión de conformidad con lo previsto en los artículos 19, 20 y 21 de la LGPDPSP.

El deber de seguridad deberá observarse durante todo el ciclo de vida de los datos personales, es decir, desde su obtención hasta su eliminación.

El ciclo de vida de los datos personales es el siguiente:



Política Interna de Protección de Datos Personales

La SHTFP deberá contar con el Documento de Seguridad correspondientes, como parte de los mecanismos implementados para asegurar el cumplimiento del deber de seguridad, cuyo objeto es describir y dar cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas, para la protección de datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

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;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad y,

VII. El programa anual de capacitación.

En las actualizaciones que se realicen al Documento de Seguridad deberán participar las personas Titulares de las Unidades Administrativas, a través de sus enlaces en materia de datos personales, quienes en todo momento observarán los principios, deberes y obligaciones a los que se refieren la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

De conformidad 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;

IV. Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Con independencia de los supuestos anteriores, el Documento de Seguridad podrá ser actualizado cada tres años.

Cuando alguna de las personas Titulares de las Unidades Administrativas se encuentre en algunos de los supuestos del artículo anterior, la o el enlace presentará por escrito a la DST las actualizaciones conducentes y está lo someterá al Comité de Transparencia para resolver lo conducente.

Trigésima séptima.- En términos de lo previsto en la Ley General, se considera como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

a) La pérdida o destrucción no autorizada;

b) El robo, extravío o copia no autorizada;

c) El uso, acceso o tratamiento no autorizado;

d) El daño, la alteración o modificación no autorizada.

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

Trigésima novena- Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de las o los titulares de los datos personales, las personas Titulares de las Unidades Administrativas involucradas, 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. Las recomendaciones dirigidas a las y los titulares;

X. El medio puesto a disposición del o la titular para que pueda obtener mayor información sobre la vulneración y cómo proteger sus datos personales;

XI. El nombre completo de la o las personas designadas para proporcionar mayor información al Órgano garante, en caso de requerirse;

XII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Órgano garante.

Para efectos del presente numeral, se entenderá que se afectan los derechos patrimoniales de la o el titular, cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

De la misma manera, se entenderá que se afectan los derechos morales del o la titular, cuando la vulneración esté relacionada de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico o menoscabe ilegalmente la libertad, integridad física o psíquica de la titular de los datos.

Cuadragésima.- Las personas Titulares de las Unidades Administrativas tendrán la obligación de notificar a la(s) persona(s) titular(es) afectada(s) la información descrita en lo incisos anteriores, a través del medio que se establezca para ese fin.

En aquellos casos en los cuales no sea posible notificar directamente a la(s) personas (s) titular(es) afectada(s) sobre el informe a que hace referencia la presente Política o ello implique esfuerzos desproporcionados, se instrumentarán medidas compensatorias de comunicación para tal efecto, como son: Aviso en la página oficial de Internet, sitios de internet, plataformas, tarjetas o cápsulas informativas u otro similar.

Con independencia de lo anterior la persona Titular de la Unidad Administrativa, deberá sujetarse a lo señalado en el artículo 31 de la Ley General, que establece que, en caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Cuadragésima primera.- El informe al que se refiere el numeral 39° de la presente Política, se deberá remitir al oficial de protección de datos personales en un plazo no mayor de cuarenta y ocho horas hábiles posteriores a que se haya confirmado la vulneración de seguridad, para que ésta la haga en tiempo y forma, de conformidad con la Ley General, los Lineamientos Generales y demás normativa aplicable.

Cuadragésima segunda.- En términos de lo previsto en el numeral anterior, el oficial de protección de datos personales deberá informar al Comité de Transparencia de lo ocurrido en torno a la vulneración de seguridad de datos personales.

El Comité de Transparencia podrá determinar la implementación de acciones adicionales a las realizadas por las personas Titulares de las Unidades Administrativas para evitar futuras vulneraciones y reforzar las medidas de seguridad existentes.

El Comité de Transparencia podrá auxiliarse de la asesoría, orientación o apoyo de las personas Titulares de las Unidades Administrativas, en asuntos de su especialidad, con la finalidad de garantizar la efectiva protección de los datos personales.

Para llevar acabo lo anterior, el Comité de Transparencia se apoyará del Oficial de Protección de Datos Personales para llevar a cabo dichas gestiones ante las personas Titulares de las Unidades de Administrativas.

Cuadragésima tercera.- La SHTFP deberá contar con un Programa de Protección de Datos Personales aprobado por el Comité de Transparencia, cuyo objetivo serán los siguientes:

I. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión de la SHTFP;

II. Cumplir con los principios, deberes y obligaciones de la Ley General, la presente Política y la normatividad que derive de los mismos;

III. Establecer 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;

IV. Promover la adopción de mejores prácticas en la protección de datos personales.

Cuadragésima cuarta. - El Programa de Protección de Datos Personales deberá estar actualizado, sin demerito de que podrá ser sometido a su revisión o reajuste por parte del Comité de Transparencia, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de estimarse necesario.

Cuadragésima quinta.- El oficial de protección de datos personales tendrá las siguientes funciones en relación al Programa de Protección de Datos Personales:

I. Elaborar y coordinar el Programa en conjunto con las Unidades Administrativas que estime necesario involucrar o consultar;

II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;

III. Dar a conocer el Programa al interior del sujeto obligado;

IV. Coordinar la implementación del Programa en las Unidades Administrativas;

V. Asesorar a las Unidades Administrativas en la implementación del Programa, con el apoyo de las áreas técnicas que estime pertinente;

VI. Las demás que de manera expresa señalen el propio Programa.

Cuadragésima sexta.- Como parte de las acciones para cumplir con el principio de información, en la SHTFP se contará con los avisos de privacidad integral y su correlativo aviso de privacidad simplificado, para el tratamiento de datos personales.

Excepcionalmente, cuando dos o más tratamientos de datos personales, atiendan una misma finalidad o función, se podrá contar con un mismo aviso de privacidad, en sus dos modalidades, siempre y cuando sea posible expresar con precisión y claridad las finalidades del tratamiento de datos personales, de tal suerte que no dé lugar a incertidumbre o ambigüedad a sus titulares.

Cuadragésima séptima.- Los formatos para la elaboración de los avisos de privacidad integral y simplificado serán acordes con los elementos que establecen en la Ley General, los Lineamientos Generales y demás normatividad que resulte aplicable.

Cuadragésima octava.- En la integración y elaboración de los avisos de privacidad, las Unidades Administrativas preverán un diseño que facilite su entendimiento por parte de las y los titulares de los datos. El oficial de protección de datos personales podrá elaborar propuestas de formatos que faciliten su integración o actualización, manteniendo la homogeneidad de los elementos.

En todo momento, los Titulares de las Unidades Administrativas, deberán asegurarse que los avisos de privacidad se encuentren actualizados.

Cuadragésima novena.- Las personas Titulares de las Unidades Administrativas se asegurarán de que la información asentada en los avisos de privacidad se encuentre redactada en un lenguaje ciudadano, sencillo, claro y comprensible, considerando en todo momento el perfil de la o el titular al cual vaya dirigido, por lo que se abstendrán de:

I. Usar frases inexactas, ambiguas o vagas;

II. Incluir textos que induzcan a los y las titulares a elegir una opción en específico;

III. Marcar previamente casillas, en caso de que éstas se incluyan, para que los y las titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que los y las titulares ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte;

IV. Remitir a textos o documentos que no estén disponibles para las y los titulares.

Quincuagésima.- La SHTFP contará 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 cumple con el principio de responsabilidad, el cual considerará los niveles de capacitación atendiendo los roles y las responsabilidades de las personas servidoras públicas que tratan datos personales.

Quincuagésima primera.- El Comité de Transparencia será el órgano encargado de aprobar el Programa de Capacitación y Actualización en la materia, con base en la propuesta que sea presentada por el oficial de protección de datos personales, en la cual se consideren las necesidades de capacitación de las Unidades Administrativas.

Quincuagésima segunda.- El oficial de protección de datos personales coordinará y dará seguimiento a los programas de capacitación continua y especializada en la materia de protección de datos personales.

Capítulo V

Ejercicio de los derechos ARCOP de los datos personales.

Quincuagésima tercera.- Para efectos de la presente Política, los Derechos ARCOP son aquellos derechos que tiene el o la titular de los datos personales, para solicitar el Acceso, Rectificación, Cancelación, Oposición y Portabilidad sobre el tratamiento de sus datos.

- Acceso: Derecho del o la titular para acceder a sus datos personales y conocer la información relacionada con las condiciones y generalidades del tratamiento.

- Rectificación: Derecho del o la titular para solicitar la corrección de sus datos personales, cuando éstos resulten inexactos, incompletos o no se encuentren actualizados.

- Cancelación: Derecho del o la titular para solicitar que sus datos personales sean bloqueados y ulteriormente suprimidos de los archivos, registros, expedientes y sistemas.
- Oposición: Derecho del o la titular para solicitar que se abstengan de solicitar información personal para ciertos fines o de requerir que se concluya el uso a fin de evitar un daño.

- Portabilidad: Es el derecho de obtener del responsable que posee los datos personales, una copia de la información que obre en sus archivos.

Quincuagésima cuarta.- .- El oficial de protección de datos personales será el responsable de turnar las solicitudes de ejercicio de derechos ARCOP que sean presentadas a la SHTFP aquellas Unidades Administrativas que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales, para que se pronuncien y den atención en los plazos y términos establecidos para la atención de Solicitudes para el Ejercicio de los Derechos ARCOP.

Quincuagésima quinta.- Cuando los datos personales se encuentren en un formato estructurado y comúnmente utilizado podrá proceder la portabilidad de los datos personales.

La Portabilidad de los datos personales, tiene por objeto que la o el titular solicite, lo siguiente:

I. Una copia de sus datos personales que hubiere facilitado directamente a la SHTFP de una Unidad Administrativa, en un formato estructurado comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otro sujeto obligado para su reutilización y aprovechamiento en un nuevo tratamiento;

II. La transmisión de sus datos personales a un sujeto obligado receptor, siempre y cuando sea técnicamente posible, la o el titular hubiere facilitado directamente sus datos personales a la SHTFP y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

Capítulo VI

De las remisiones y transferencias de los datos personales

Quincuagésima sexta.- Se le conoce como remisión, a toda comunicación de datos personales realizada por la persona Titular de la Unidad Administrativa y la o el encargado dentro y fuera del territorio mexicano.

La figura de la o el encargado, es una persona prestadora de servicios que trata datos personales a nombre de la persona Titular de la Unidad Administrativa responsable de los datos personales.

La o el encargado, tiene las siguientes características: puede ser una persona física o jurídica, de ámbito público o privado, ajeno a la SHTFP, puede ser una sola persona o de manera conjunta con otras personas, no tiene poder de decisión sobre el alcance y contenido del tratamiento de los datos personales y debe delimitar sus actuaciones a lo que diga la persona Titular de la Unidad Administrativa responsable de los datos personales.

Quincuagésima séptima.- La transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta de la o el titular, de la persona Titular de la Unidad Administrativa o la o el encargado.

Toda transferencia de datos personales se encontrará sujeta al consentimiento de su titular. Para tal efecto, a través del aviso de privacidad correspondiente informarán al o la titular de los datos personales, las finalidades de la transferencia, así como el tercero receptor.

No se requerirá el consentimiento de la o el titular para llevar a cabo la transferencia de sus datos personales, en los casos previstos en los artículos 16, 59 y 64 de la LGPDPPSO.

Capítulo VII

Supervisión en materia de protección de datos personales

Quincuagésima octava.- Para el debido cumplimiento de los principios, deberes y obligaciones que establecen la Ley General y la normativa aplicable en materia de Unidades Administrativas para garantizar el derecho a la protección de datos personales en la SHTFP de conformidad con lo dispuesto en el artículo 78 fracción I de la Ley General.

Quincuagésima novena.- La supervisión en materia de protección de datos personales se sustanciará mediante requerimientos de información sobre el tratamiento de datos personales, así como de sugerencias a las Unidades Administrativas para prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

Transitorios

PRIMERO.- La presente Política entrará en vigor a partir de su aprobación por el Comité de Transparencia de la Secretaría de Honestidad, Transparencia y Función Pública.

SEGUNDO.- Notifíquese la presente Política a las personas Titulares de las Unidades Administrativas a través del oficial de protección de datos personales de la SHTFP, difúndase al interior de la SHTFP y publíquese en el sitio oficial de Internet de la Secretaría.

TERCERO.- El oficial de protección de datos personales deberá elaborar y coordinar en conjunto con las Unidades Administrativas el Programa de Protección de Datos Personales y ser aprobado por el Comité de Transparencia de la SHTFP.

Aprobación

La presente Política Interna de Protección de Datos Personales de la Secretaría de Honestidad, Transparencia y Función Pública fue aprobada por el Comité de Transparencia en su Cuarta Sesión Ordinaria del ejercicio fiscal 2025, celebrada el 30 de julio de 2025, al ser la autoridad máxima en materia de protección de datos personales de conformidad a los artículos 24, fracción II, 77, 78, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Elaboró: Lic. Armando Sánchez Pineda, Jefe de Departamento de Gobierno Abierto y Oficial de Protección de Datos Personales.

Autorizó. Lic. Carlos Alberto Deheza Figueroa, Director de Transparencia, Ética e Integridad Pública y Responsable de la Unidad de Transparencia.