



Programa de Protección de datos personales

**Servicio de Administración
Tributaria
2025 - 2026**

↓
9
K



Índice

Contenido

1. Glosario de Términos Comunes	3
2. Presentación.....	6
3. Objetivos del Programa	7
4. Responsabilidades dentro del Programa	7
5. Alcance del Programa.....	7
6. Política de Gestión de los Datos Personales	8
6.1 Inventario de tratamientos de datos personales	8
6.2 Cumplimiento de Obligaciones	11
6.2.1 Obligaciones Transversales	11
6.2.2 Obligaciones relevantes en la etapa de OBTENCIÓN de los datos personales.....	14
6.2.3 Obligaciones relevantes en la etapa de USO de los datos personales	30
6.2.4 Obligaciones relevantes en la etapa de ELIMINACIÓN de los datos personales	48
6.2.5 Otras Obligaciones	50
7. Sanciones por Incumplimiento	60

1
9
2



1. Glosario de Términos Comunes

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, 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: Instancia a la que hace referencia el artículo 39 de la Ley General de Transparencia y Acceso a la Información Pública.

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

Datos personales sensibles: Aquellos que se 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 o morales y opiniones.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

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

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

Evaluación de impacto en la protección de datos personales: Evaluación mediante la 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, valoran 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.

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

I
d
✓



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.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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:

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Portabilidad de datos personales: Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

Programa: Programa de Protección de Datos Personales.

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

Responsable: Sujeto obligado de la LGPDPSO que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.



Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

SAT: Servicio de Administración Tributaria.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: Persona física a quien corresponden los datos personales.

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

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

Unidad Administrativa: Área a la que se le confieren atribuciones específicas en el Reglamento Interno del SAT.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 41 de la Ley General de Transparencia y Acceso a la Información Pública.

↓
9
2



2. Presentación

De conformidad con el artículo 28 de la LGPDPSO, un sistema de gestión es un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

El sistema de gestión¹ en el que se basa esta Guía desarrolla las siguientes cuatro fases: planificar, hacer, verificar y actuar (PHVA), de acuerdo con lo descrito en la tabla siguiente:

	Elemento	Fase del ciclo PHVA	Actividades
PROCESO	Metas	Planificar	Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado (meta).
	Medios de acción	Hacer	Implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
	Seguimiento	Verificar	Evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y el logro de la mejora esperada.
	Acciones correctivas	Actuar	Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión realizada, o de otra información relevante, para lograr la mejora continua.

¹ El ciclo PHVA (Planificar, Hacer, Verificar, Actuar), también conocido como ciclo de Deming, es una metodología de gestión para la mejora continua de procesos y productos.

ACTUAR
Adoptar medidas correctivas y preventivas en función de los resultados y de la revisión realizada, o de otra información relevante, para lograr la mejora continua

VERIFICAR
Evaluar y medir los resultados de lo implementado, a fin de verificar el adecuado funcionamiento del sistema de gestión y el logro de la mejora esperada.



PLANIFICAR
Identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por el responsable o encargado (meta).

HACER
Implementar y operar las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior

R 9



Para la elaboración del presente documento, se identificaron las obligaciones que establece la LGPDPPSO y la normativa aplicable en materia de protección de datos personales para todo sujeto obligado y, a partir de ello, se definieron las acciones a seguir para su cumplimiento.

3. Objetivos del Programa

El presente programa tiene como objetivos los siguientes:

- Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del SAT;
- Cumplir con las obligaciones que establece la LGPDPPSO y la normativa aplicable en materia de protección de datos personales;
- Establecer los elementos y 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, y
- Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la organización, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

4. Responsabilidades dentro del Programa

Las unidades administrativas y la Unidad de Transparencia tendrán las funciones y responsabilidades descritas en el presente Programa.

Para que la implementación del Programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LGPDPPSO y la normativa aplicable en materia de datos personales, éste será de observancia obligatoria para todas las personas servidoras públicas del SAT que en el ejercicio de sus funciones traten datos personales.

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

Para ello, resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que deberá ser difundido entre las personas servidoras públicas.

5. Alcance del Programa

El presente Programa aplicará a todas las unidades administrativas del SAT que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones. Asimismo, en virtud de que uno de los objetivos

1
9
4



del Programa es cumplir con las obligaciones establecidas en la LGPDPPSO, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento².

Las unidades administrativas que forman parte del SAT, de conformidad con el Reglamento Interior del SAT, deberán observar el presente Programa.

6. Política de Gestión de los Datos Personales

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la LGPDPPSO, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO y la normativa en materia de protección de datos personales, y según el ciclo de vida de los datos personales.

Asimismo, el SAT procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.

6.1 Inventario de tratamientos de datos personales

Para el debido cumplimiento de las obligaciones que se establecen en el apartado 6.2 de este programa, es necesario que cada una de las unidades administrativas realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en el SAT.

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del SAT, realizado con orden y precisión.

El inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 27, fracción III, 29, fracción I, identificará los siguientes elementos relevantes:

1. ¿Qué tratamientos de datos personales realiza la unidad administrativa?

Hay que identificar cada uno de los procesos en los que la unidad administrativa trata datos personales.

² Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 56 de la Ley General de Transparencia y Acceso a la Información Pública.



2. ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos?

Hay que identificar o definir si la unidad administrativa está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.

Podría ocurrir que una unidad administrativa trate datos personales recabados en el marco de un proceso del cual no es responsable. Por ejemplo, con motivo de una consulta, la unidad administrativa "X" podría tener acceso a datos de contacto del particular que realizó la consulta, sin embargo, la unidad administrativa que está a cargo del procedimiento de atención a consultas, y quien administra la base de datos de las consultas que recibe la institución es la unidad administrativa "Y".

Asimismo, podría darse el caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

En ese sentido, para definir quién está a cargo del proceso mediante el cual se recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes, es necesario analizar la función que realiza cada unidad administrativa dentro del proceso, y las atribuciones o facultades normativas que resulten aplicables.

3. Una vez que hayan sido identificados los tratamientos de los cuales está a cargo la unidad administrativa, será necesario determinar lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

a) ¿Cómo se obtienen los datos personales?

- Directamente del titular
 - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.
 - Vía telefónica.
 - Por correo electrónico.
 - Por Internet o sistema informático.
 - Por escrito presentado directamente en las oficinas del sujeto obligado.
 - Por escrito enviado por mensajería.
- Mediante una transferencia
 - Medios por los que se realiza la transferencia.
- De una fuente de acceso público

b) ¿Qué tipo de datos personales se tratan? ¿son sensibles?

c) ¿Dónde se almacenan y realiza el tratamiento de los datos personales?

- Sección, serie y subserie de archivos
- Formato en que se encuentra la base de datos: físico y/o electrónico
- Ubicación de la base de datos.

1

9

✓



d) ¿Para qué finalidades se utilizan los datos personales?

Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales. Por ejemplo, el procedimiento podría ser "contratación de personal" y las finalidades "evaluación de currículum para la selección de personal".

Será necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir qué supuestos (fracciones) del artículo 16 de la LGPDPSO se actualizan.

Asimismo, se deberá señalar el marco jurídico que da facultades para el tratamiento de datos personales (disposición normativa, artículo, fracción, inciso, párrafo).

e) ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado?

Se deberá identificar el catálogo de personas servidoras públicas al interior del SAT que tienen acceso a los datos personales y para qué fin.

f) ¿Intervienen encargados en el tratamiento de los datos personales?

Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente.

g) ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?

Hay que identificar las autoridades o terceros externos al SAT a quienes se comunican los datos personales y los fines de las transferencias.

Asimismo, es necesario señalar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se requiera el consentimiento, se deberá definir qué supuestos (fracciones) de los artículos 16 y 64 de la LGPDPSO se actualizan.

h) ¿Se difunden los datos personales?

Hay que señalar si los datos personales se difunden y el fundamento jurídico para ello.

i) ¿Cuál es el plazo de conservación de los datos personales?

Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

Una vez que se haya realizado este diagnóstico inicial, estaremos preparados para cumplir de mejor manera con las obligaciones previstas en la LGPDPSO y la normativa en materia de protección de datos personales.



6.2 Cumplimiento de Obligaciones

En la presente sección se identificarán las obligaciones que establecen la LGPDPPSO y la normativa en materia de protección de datos personales y se dividirán según las distintas etapas del ciclo de vida de los datos personales (obtención, uso y eliminación), señalando la siguiente información:

- Descripción de las obligaciones
- Actividades a realizar para cumplirlas
- Artículos de la LGPDPPSO y la normativa en materia de protección de datos personales de los que derivan
- Unidad administrativa responsable del cumplimiento
- Listado de comprobación del estado de cumplimiento

La etapa de obtención de los datos personales se identificará con la letra "O", la de uso con la "U", la de eliminación con la "E", y las transversales con la "T", para fácil referencia.

Si bien, las obligaciones se dividieron según el ciclo de vida de los datos personales con fines de claridad y orden, es importante señalar que es ineludible cumplir con todos los principios y deberes que establecen la LGPDPPSO, y la normativa en materia de protección de datos personales que resulte aplicable, en cualquier momento del tratamiento o ciclo de vida de los datos personales.

6.2.1 Obligaciones Transversales

Los deberes de seguridad y confidencialidad deben observarse especialmente en cualquier etapa del ciclo de vida de los datos personales.

1.T. MEDIDAS DE SEGURIDAD

El deber de seguridad consiste en la implementación de medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no automatizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

T

1



Las medidas de **seguridad administrativas** refieren a las 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.

Por su parte, las medidas de **seguridad físicas** son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Asimismo, las medidas de **seguridad técnicas** abarcan el 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.

2.T. DOCUMENTO DE SEGURIDAD

Por otra parte, de conformidad con el artículo 29 de la LGPDPSO, el responsable deberá elaborar un documento de seguridad, el cual deberá contener, al menos, la siguiente información:

- 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 general de capacitación

3.T. VULNERACIONES

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

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



4.T. CONFIDENCIALIDAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
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.	1. Incluir en las medidas de seguridad, controles para garantizar la confidencialidad de los datos personales.	Unidad administrativa encargada de la seguridad de la información al interior de la institución.	<ul style="list-style-type: none"> Documento de seguridad. Controles definidos para la confidencialidad de los datos personales.
	2. 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.	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> Evidencia de la aplicación de los controles.
	3. Establecer cláusulas en los contratos con los encargados, que obliguen a la confidencialidad de los datos personales.	Unidad administrativa competente.	<ul style="list-style-type: none"> Contratos celebrados con los encargados del tratamiento.
	4. Implementar capacitación para las personas servidoras públicas del SAT, a fin de generar conciencia sobre la importancia de guardar la confidencialidad de los datos personales que tratan.	Comité de Transparencia y unidad administrativa competente.	<ul style="list-style-type: none"> Documentación que acredite la capacitación brindada y tomada.

Artículos vinculados: 30 LGPDPPSO.

NOTA: Este deber deberá observarse durante todo el ciclo de vida de los datos personales, desde su obtención hasta su eliminación

T

1



6.2.2 Obligaciones relevantes en la etapa de OBTENCIÓN de los datos personales

1.0. LICITUD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Sujetar el tratamiento de los datos personales a las atribuciones o facultades que la normatividad aplicable confiera al sujeto obligado, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.	Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> Marco normativo aplicable.

Artículos vinculados: 11 de la LGPDPSO.

↓
→
g

2.O. LEALTAD			
Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
No obtener ni tratar los datos personales a través de medios engañosos o fraudulentos.	1. Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.	Todas las unidades administrativas que realicen tratamiento de datos personales.	• Medios para la obtención de los datos personales.
Privilegiar los intereses y expectativa razonable de privacidad de los titulares.	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. Ver obligación 3.O. 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. Ver obligación 3.O. 5. Llevar a cabo el tratamiento de los datos personales sólo para los fines informados en el aviso de privacidad.	Todas las unidades administrativas que realicen tratamiento de datos personales.	• Avisos de privacidad.

Artículos vinculados: 13 de la LGPDPPSO

NOTA: Esta obligación deberá observarse a lo largo de todo el ciclo de vida de los datos personales, desde la obtención de los mismos hasta su tratamiento y eliminación.



3.0. INFORMACIÓN (AVISO DE PRIVACIDAD)

Uno de los elementos fundamentales para que los titulares de los datos personales puedan ejercer su derecho a la protección de sus datos personales es conocer la existencia y características principales del tratamiento al que serán sometidos sus datos personales, entre ello, quién es el responsable del tratamiento, para qué fines se utilizarán los datos personales, con quién se compartirán, cómo ejercer los derechos de acceso, rectificación, cancelación oposición (derechos ARCO) y portabilidad.

De hecho, una condición necesaria para que el consentimiento del tratamiento de datos personales sea válido, es que éste sea informado, lo que implica que el titular conozca el aviso de privacidad previo a la manifestación de su voluntad.

El aviso de privacidad es el documento mediante el cual se materializa el principio de información, y en el cual se dan a conocer las características principales del tratamiento de los datos personales, a través de los elementos informativos que establece la LGPDPSO.

En ese sentido, el principio de información se constituye en el derecho de los titulares para conocer las características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad y, a su vez, en una obligación para el responsable de poner a disposición de los titulares dicho aviso.

Para cumplir con el principio de Información se deberán seguir las siguientes reglas:

1. Redactar los avisos de privacidad que se requieran conforme a los tratamientos que lleven a cabo las unidades administrativas. Como regla general, se requerirá un aviso de privacidad por tratamiento. Sólo en los casos en que la información a incluir en el aviso de privacidad de distintos tratamientos sea la misma en su mayoría, se podrá redactar un aviso de privacidad común. El criterio para este supuesto es que la redacción del aviso de privacidad compartido no sea confusa.
2. Seguir el formato establecido por el Comité de Transparencia para homologar los avisos de privacidad al interior del SAT, para facilitar su entendimiento por parte de los titulares.
3. Elaborar las dos modalidades para cada aviso de privacidad: simplificado e integral.
4. Poner a disposición todos los avisos de privacidad, en sus modalidades simplificada e integral, en el portal de Internet del SAT, en la sección que se destine para ello, a fin de que se difunda por medios electrónicos.

De manera adicional, los avisos de privacidad deberán estar disponibles para su consulta en medio impreso (físico) en las instalaciones del SAT, en donde resulte conveniente según el medio por el que se obtengan los datos personales y por el que se tenga contacto con los titulares.





Asimismo, cuando ello sea necesario o conveniente, el aviso de privacidad se podrá dar a conocer por otros formatos y medios, como por ejemplo en formato sonoro, vía telefónica, entre otros.

- Implementar mecanismos para dar a conocer el aviso de privacidad en los momentos antes señalados, según sea el caso.
- Poner a disposición el aviso de privacidad simplificado en un primer momento, de manera preferente.

4.O. MEDIDAS COMPENSATORIAS

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Instrumentar medidas compensatorias cuando resulte imposible dar a conocer al titular el aviso de privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados, de acuerdo con los Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.	1. Dar a conocer el aviso de privacidad simplificado a través de la implementación de medidas compensatorias cuando i) resulte imposible dar a conocer al titular el aviso de privacidad de manera directa, o ii) ello exija esfuerzos desproporcionados.	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> • Evidencia de la difusión del aviso de privacidad por el medio de comunicación masiva utilizado para la medida compensatoria implementada. • En su caso, autorización del SABG y evidencia de su difusión.
Las medidas compensatorias son mecanismos alternos para dar a conocer a los titulares el aviso de privacidad simplificado, a través de su difusión por medios masivos de comunicación u otros mecanismos de amplio alcance, como los siguientes:	2. Evaluar si se requiere o no la autorización expresa de la SABG para la implementación de medidas compensatorias.	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> • Evidencia de la difusión del aviso de privacidad por el medio de comunicación masiva utilizado para la medida compensatoria implementada.



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<ul style="list-style-type: none"> • Diario Oficial de la Federación o diarios de circulación nacional; o • Diarios o gacetas oficiales de las entidades federativas, o diarios de circulación regional o local, o bien, revistas especializadas; o • Página de Internet o cualquier otra plataforma o tecnología oficial del responsable; o • Carteles informativos; o • Cápsulas informativas radiofónicas, o • Cualquier otro medio alternativo de comunicación masivo. 			<ul style="list-style-type: none"> • En su caso, autorización del SABG y evidencia de su difusión.

Artículos vinculados: 20 de la LGPDPSO, instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.

1

g

7

5.O. CONSENTIMIENTO

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del Cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Contar con el consentimiento del titular, para el tratamiento de sus datos personales, salvo que se actualice alguna de las excepciones previstas en el artículo 16 de la LGPDPSO, que señala lo siguiente:</p> <p>Artículo 16. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:</p> <p><i>I. Cuando una legislación aplicable así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, y en ningún caso podrán contravenirla;</i></p> <p><i>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</i></p>	<p>1. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.</p> <p>2. En esos casos, solicitar el consentimiento de los titulares según las reglas que se definen a continuación.</p>	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Consentimiento expreso otorgado por los titulares y la solicitud respectiva. • Aviso de privacidad y procedimiento para su puesta a disposición.



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del Cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p><i>finalidad que motivó el tratamiento de los datos personales;</i></p> <p>III. <i>Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;</i></p> <p>IV. <i>Para el reconocimiento o defensa de derechos de la persona titular ante autoridad competente;</i></p> <p>V. <i>Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y el responsable;</i></p> <p>VI. <i>Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;</i></p> <p>VII. <i>Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;</i></p>			

↓

o

2



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del Cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>III. Cuando los datos personales figuren en fuentes de acceso público;</p> <p>IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o</p> <p>X. Cuando la persona titular de los datos personales sea una persona reportada como desaparecida en los términos de las disposiciones jurídicas en la materia.</p> <p>La actualización de alguno de los supuestos anteriores no exime al responsable del cumplimiento de las demás obligaciones establecidas en la LGPDPPSO</p>			
<p>El consentimiento que, en su caso, se obtenga debe ser libre, específico e informado, según lo dispuesto por el artículo 14 de la LGPDPPSO:</p> <p>Artículo 14. Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 16 de la presente Ley, el responsable deberá contar con el consentimiento previo de la persona titular para el</p>	<p>3. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.</p> <p>4. 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, y se distingan de asuntos ajenos a la</p>	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Aviso de privacidad. • Texto de solicitud de consentimiento.

1



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del Cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p><i>tratamiento de los datos personales, el cual deberá otorgarse de forma:</i></p> <p><i>I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad de la persona titular;</i></p> <p><i>II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, y</i></p> <p><i>III. Informada: Que la persona titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales. En la obtención del consentimiento de personas menores de edad o que se encuentren en estado de interdicción o incapacidad declarada conforme a las disposiciones jurídicas aplicables, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.</i></p>	<p>protección de datos personales, cuando ello sea necesario.</p> <p>5. 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.</p> <p>6. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso, en los términos señalados en la columna anterior, así como documentar su obtención.</p> <p>7. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.</p>	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Solicitud del consentimiento expreso. • Consentimiento expreso otorgado por los titulares. • Puesta a disposición del aviso de privacidad.

1

g

2



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del Cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Por otra parte, la solicitud del consentimiento deberá ser concisa e inteligible, estar redactada en un lenguaje claro y sencillo y, cuando se refiera a diversos asuntos ajenos a la protección de datos personales, deberá presentarse de tal forma que se distinga claramente de dichos asuntos.</p> <p>Dependiendo del tipo de datos personales, el consentimiento deberá ser tácito o expreso, siguiendo las reglas establecidas en el artículo 15 de la LGPDPPSO:</p> <p>Artículo 15. <i>El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad de la persona titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.</i></p> <p><i>El consentimiento será tácito cuando habiéndose puesto a disposición de la persona titular el aviso de privacidad, ésta no</i></p>			

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del Cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p><i>manifieste su voluntad en sentido contrario.</i></p> <p><i>Por regla general será válido el consentimiento tácito, salvo que las disposiciones jurídicas aplicables exijan que la voluntad de la persona titular se manifieste expresamente.</i></p> <p><i>Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito de la persona 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 esta Ley.</i></p>			
<p>Cuando los datos personales se obtengan indirectamente del titular, y se requiera el consentimiento, no se podrán tratar los datos personales hasta que se cuente con la manifestación libre, específica e informada del titular, en la que autorice el tratamiento de sus datos</p>	<p>8. Cuando los datos personales no los proporcione personal o directamente el titular o su representante, el sujeto obligado deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado.</p>	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Aviso de privacidad. • Constancia de envío del aviso de privacidad. Se sugiere utilizar un medio que permita acreditar la fecha en la que el titular recibió el aviso de privacidad. • Respuesta por parte de los titulares.

1

g

2

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del Cumplimiento	Medios que facilitan la acreditación del cumplimiento
personales de manera tácita o expresa, según corresponda.	<p>Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento.</p> <p>Si el titular no manifiesta su negativa en el plazo de cinco días antes señalado, el sujeto obligado podrá suponer que cuenta con el consentimiento tácito.</p> <p>En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte.</p> <p>El sujeto obligado no podrá tratar los datos personales si no cuenta con el consentimiento expreso del titular.</p>		<ul style="list-style-type: none"> Consentimiento expreso otorgado.
Atender, de ser el caso, las solicitudes de revocación del consentimiento, mismas que podrán ser presentadas por el titular en cualquier momento del tratamiento sin que se le atribuyan efectos retroactivos, a través del ejercicio de los derechos de oposición y cancelación.	9. Prever lo relativo a la revocación del consentimiento, según los plazos, requisitos y procedimiento que se establecen para el ejercicio de los derechos de cancelación y oposición.	Comité de Transparencia y Unidad de Transparencia.	<ul style="list-style-type: none"> Procedimiento Interno atención derechos ARCO.

Artículos vinculados: 14, 15 y 16 de la LGPDPSO.

6.O. CONSENTIMIENTO MENORES DE EDAD Y PERSONAS EN ESTADO DE INTERDICCIÓN O INCAPACIDAD DECLARADA CONFORME A LA LEY

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Atender las reglas de representación previstas en el Código Civil Federal y demás disposiciones que resulten aplicables en la materia específica de que se trate, para la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley.</p>	<ol style="list-style-type: none"> 1. Identificar los tratamientos de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, que requieren consentimiento, según el artículo 14 de la LGPDPSO. 2. Poner a disposición de los padres, tutores o representantes legales el aviso de privacidad, así como también, cuando ello sea posible, a los menores de edad y al titular en estado de interdicción o incapacidad declarada conforme a ley. 3. Redactar los avisos de privacidad y solicitudes de consentimiento en lenguaje sencillo, adaptado para la comprensión del menor de edad o de la persona que se encuentre en estado de interdicción o incapacidad declarada conforme a ley. 4. Implementar mecanismos que permitan tener certeza que quien otorga el consentimiento, está facultado legalmente para ello, máxime cuando el mismo no se vaya a requerir con la presencia física de los padres, tutores o representantes legales. 	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Documentación que acompañe la solicitud y el otorgamiento del consentimiento por parte de los padres, tutores o representantes legales.

Artículos vinculados: 14 de la LGPDPSO.

↓

o

z



7.O. DATOS PERSONALES SENSIBLES

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
No tratar datos personales sensibles, salvo que se cuente con el consentimiento expreso del titular o se trate de los casos establecidos en el artículo 16 de la LGPDPPSO.	<p>1. Revisar la necesidad y legalidad del tratamiento de datos personales sensibles para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada su obtención y uso.</p> <p>2. Revisar que se actualice alguno de los supuestos del artículo 16 de la LGPDPPSO, o bien, en caso contrario, solicitar el consentimiento expreso y por escrito del titular.</p>	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> Marco normativo que habilita para el tratamiento de datos personales sensibles. Consentimiento del titular, en su caso, o la actualización de alguno de los supuestos previstos en el artículo 16 de la LGPDPPSO.
No llevar a cabo tratamiento de datos personales que tengan como efecto la discriminación de los titulares por su origen étnico o racial, su estado de salud presente, pasado o futuro, su información genética, sus opiniones políticas, su religión o creencias filosóficas o morales y su preferencia sexual.	3. Verificar que el tratamiento de datos personales no tenga como consecuencia discriminación de los titulares.	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> Documentación que se genere en torno al tratamiento.

Artículos vinculados: 16 de la LGPDPPSO.



8.O. INTERÉS SUPERIOR DE LOS MENORES DE EDAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Privilegiar el interés superior del niño, niña y adolescente en el tratamiento de sus datos personales, en términos de las disposiciones previstas en la Ley General de los Derechos de Niñas, Niños y Adolescentes, así como lo dispuesto en la Ley General.</p> <p>Esta obligación se deberá observar en todo el ciclo de vida de los datos personales, desde la obtención de los datos personales de menores de edad, hasta su tratamiento y cancelación.</p>	<ol style="list-style-type: none"> 1. En todos los casos en que estén involucrados datos personales de menores de edad, tener siempre en cuenta y privilegiar el interés superior del menor de edad. 2. Conocer la Ley General de Niñas, Niños y Adolescentes, con objeto de conocer los derechos de los menores de edad y las obligaciones al respecto. 3. Poner a disposición el aviso de privacidad tanto al adulto que tenga la representación del menor, como al propio titular de los datos personales. 4. Solicitar el consentimiento del adulto que tenga la representación del menor, cuando éste se requiera, y de manera adicional solicitar la opinión del propio titular. 	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Documentación o procedimiento que acredite la puesta a disposición del aviso de privacidad al adulto que tenga la representación del menor de edad y al propio titular de los datos personales. • Documento que acredite la obtención del consentimiento del adulto que tiene la representación del menor, así como la opinión del propio titular.

Artículos vinculados: 7 de la LGPDPPSO.

9.O. PROPORCIONALIDAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Tratar los datos personales sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.</p>	<ol style="list-style-type: none"> 1. Identificar qué datos personales se requieren para cada una de las finalidades. El listado de datos personales debe estar completo con independencia de que en el 	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Avisos de privacidad- • Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico-

1

9

2

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas al responsable por la normativa en la materia.	<p>aviso de privacidad se informe por categoría de datos.</p> <p>2. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.</p> <p>3. Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.</p>		
Realizar esfuerzos razonables para limitar los datos personales tratados, al mínimo necesario, con relación a las finalidades que motivaron su tratamiento.	4. Requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> • Avisos de privacidad. • Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.

Artículos vinculados: 12 de la LGPDPSO.

6.2.3 Obligaciones relevantes en la etapa de USO de los datos personales

1.U. FINALIDAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Justificar el tratamiento de los datos personales en finalidades concretas, lícitas, explícitas y legítimas. Se entenderá que las finalidades son:</p> <p>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 el titular;</p> <p>II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;</p> <p>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</p> <p>IV. 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</p>	<ol style="list-style-type: none"> 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 según las reglas descritas anteriormente. 		

↓
g

✓



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
el artículo 12 de la LGPDPSO.			
Las finalidades deben estar relacionadas con las atribuciones normativas de la unidad administrativa que realice el tratamiento.	4. Identificar el marco normativo (ley, reglamento, lineamiento, entre otros, con sus respectivos artículos) que otorga las atribuciones a la unidad administrativa para tratar los datos personales para cada una de las finalidades	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> Marco normativo.
<p>Cuando se vayan a tratar los datos personales para finalidades distintas a las previstas en el aviso de privacidad, se requiere tener atribuciones legales para ello y el consentimiento del titular, salvo que se trate de una persona desaparecida.</p> <p>Se deberá considerar:</p> <p>I. La expectativa razonable de privacidad del titular, basada en la relación que tiene con éste;</p> <p>II. La naturaleza de los datos personales;</p> <p>III. Las consecuencias del tratamiento posterior de los datos personales para el titular, y</p> <p>IV. Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la LGPDPSO.</p>	<p>5. Identificar las finalidades que no fueron informadas en los avisos de privacidad y que se requieran llevar a cabo.</p> <p>6. Verificar que existan atribuciones legales para el tratamiento de los datos personales para estas finalidades adicionales.</p> <p>7. Solicitar el consentimiento de los titulares para el tratamiento de datos personales para estas finalidades adicionales, cuando el mismo se requiera.</p> <p>8. Implementar las medidas que se requieran para cumplir con las obligaciones que establece la LGPDPSO, con relación a las finalidades adicionales.</p>	Todas las unidades administrativas que realicen tratamiento de datos personales.	<ul style="list-style-type: none"> Marco normativo.

Artículos vinculados: 12 de la LGPDPSO.



2.U. CALIDAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular. Se entenderá que los datos personales son:</p> <p>I. Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad; II. Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable, y III. Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.</p>	<p>1. 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.</p> <p>Estas medidas deberán permitir que la modificación de los datos personales sea inmediata, una vez que la unidad administrativa tenga conocimiento de la actualización o corrección a que haya lugar.</p>	<p>Todas las unidades administrativas que realicen tratamiento de datos personales.</p>	<ul style="list-style-type: none"> • Base de datos actualizada y correcta • Constancias o anotaciones sobre la rectificación realizada, en aquellos casos en que la misma haya sido procedente
<p>Establecer plazos de conservación de los datos personales, los cuales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, asimismo deberán atender las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales</p>	<p>2. Establecer los plazos de conservación de los datos personales, para cada uno de los tratamientos, lo cual deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística.</p>	<p>Todas las unidades administrativas que realicen tratamiento de datos personales con el apoyo del área encargada de la materia de archivos del SAT.</p>	<ul style="list-style-type: none"> • Instrumentos de clasificación archivística.

↓
d



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Establecer y documentar los procedimientos para la conservación y supresión de los datos personales, en los cuales se incluyan los periodos de conservación, mecanismos que permitan cumplir con dichos plazos, así como realizar una revisión periódica sobre la necesidad de conservar los datos personales.	3. Elaborar los procedimientos para la conservación y supresión de los datos personales, así como documentarlos. Estos procedimientos podrán ser los establecidos en materia de archivos, si a través de los mismos se puede cumplir con la obligación prevista en la LGPDPPSO.	Unidad administrativa encargada de la materia de archivos del SAT.	<ul style="list-style-type: none">• Procedimientos desarrollados.• Documentación y evidencia que se genere con su implementación.

Artículos vinculados: 17 y 18 de la LGPDPPSO.



3.U. RELACIÓN CON LOS ENCARGADOS

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido.</p> <p>Incluir en el contrato o instrumento jurídico, al menos, las siguientes obligaciones del encargado:</p> <ul style="list-style-type: none"> *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 o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales; 	<p>1. Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que contenga las obligaciones y cláusulas antes señaladas.</p>	<p>Unidad administrativa competente.</p>	<ul style="list-style-type: none"> •Cláusula tipo. •Contratos o instrumentos jurídicos.

1
o



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>* 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;</p> <p>* Permitir a la SABG o al responsable, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales;</p> <p>* Colaborar con la SABG en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPSO y</p> <p>* Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.</p>			
<p>Autorizar las subcontrataciones que realicen los encargados y que involucren el tratamiento de datos personales.</p> <p>Informar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones antes señaladas.</p>	<p>2. Incluir en los contratos originales con los encargados una cláusula que haga referencia a lo que procederá en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales.</p> <p>En el contrato original se podrá autorizar o prohibir de manera directa la subcontratación de este tipo de servicios, o bien, se podrá establecer que para la</p>	<p>Unidad administrativa competente.</p>	<ul style="list-style-type: none"> • Cláusula tipo. • Contratos o instrumentos jurídicos.



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
	<p>subcontratación será necesario que el encargado solicite autorización expresa al responsable, caso por caso. Las autorizaciones se podrán otorgar desde el contrato original, cuando el encargado ya prevea subcontrataciones específicas, y garantice que las mismas se realizarán en las condiciones antes señaladas.</p> <p>En caso contrario, la autorización se realizará de manera posterior. Para el cumplimiento de esta obligación, es necesario que el contrato o el instrumento jurídico, celebrado de origen con el encargado, establezca que las subcontrataciones que no se establezcan de manera expresa en dicho contrato o instrumento deberán ser autorizadas por el responsable. Asimismo, si se van a autorizar las subcontrataciones o quedará abierta dicha posibilidad, será necesario que, en el contrato original entre el responsable y el encargado, se establezca que si este último pretende llevar a cabo subcontrataciones deberá suscribir un contrato o instrumento jurídico con el tercero de que se trate, en el que se deberán prever las cláusulas a las que refiere la columna anterior como parte de las obligaciones del subcontratado.</p>		

Artículos vinculados: 53 y 55 de la LGPDPSO.

A
D
2



4.U. CÓMPUTO EN LA NUBE

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Contratar servicios de cómputo en la nube y similares con proveedores que garanticen políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la LGPDPSO y demás disposiciones que resulten aplicables en la materia.</p>	<p>1. Verificar las cláusulas contractuales antes de la contratación, con objeto de garantizar que el servicio cumpla con los requisitos que establece la LGPDPSO.</p>	<p>Unidad administrativa encargada de la contratación de servicios informáticos.</p>	<ul style="list-style-type: none"> • Contratos o instrumentos jurídicos.
<p>Delimitar el tratamiento de datos personales a través de cláusulas contractuales u otros instrumentos jurídicos.</p>			
<p>Contratar sólo servicios de cómputo en la nube que cumplan, al menos, con lo siguiente:</p> <ul style="list-style-type: none"> • Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LGPDPSO y demás normativa aplicable; • Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; • Abstenerse de incluir condiciones en la prestación del 	<p>2. Sólo contratar servicios de cómputo en la nube que garanticen los requisitos antes señalados.</p> <p>En caso de que los contratos se hayan celebrado antes de la entrada en vigor de la LGPDPSO, será necesario que, para su modificación o renovación, en caso de que ello fuera a ocurrir, se revise que los mismos cumplen con las condiciones antes señaladas, pues de lo contrario no podrán renovarse ni modificarse en los mismos términos.</p>		



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y</p> <ul style="list-style-type: none"> • Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio. 			
<p>Contratar sólo servicios de cómputo en la nube que cuenten con mecanismos, al menos, para:</p> <ul style="list-style-type: none"> • 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 	<p>3. Sólo contratar servicios de cómputo en la nube que garanticen los requisitos antes señalados.</p> <p>En caso de que los contratos se hayan celebrado antes de la entrada en vigor de la LGPDPPSO, será necesario que, para su modificación o renovación, se revise que los mismos cumplen con las condiciones antes señaladas, pues de lo contrario no podrán renovarse ni modificarse en los mismos términos.</p>	<p>Unidad administrativa encargada de la contratación de servicios informáticos.</p>	<ul style="list-style-type: none"> • Contratos o instrumentos jurídicos.

1

[Handwritten signature]

2



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, está obligado a informar de ese hecho al responsable.			
No contratar o adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la LGPDPSO y demás disposiciones que resulten aplicables en la materia.	(No hay actividades designadas, al ser una prohibición y no un mandato de hacer).	Unidad administrativa encargada de la contratación de servicios informáticos.	<ul style="list-style-type: none"> • Contratos o instrumentos jurídicos.
<p>Cuando el responsable tenga la posibilidad de convenir con el proveedor las condiciones y términos del servicio, además de observar las obligaciones antes señaladas -específicas para servicios de cómputo en la nube-, se deberá incluir en el contrato o instrumento jurídico las obligaciones generales de cualquier encargado:</p> <ul style="list-style-type: none"> • 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; 	4. En su caso, incluir en el contrato o instrumento jurídico que formalice la contratación de los servicios, las obligaciones generales de cualquier encargado.	Unidad administrativa encargada de la contratación de servicios informáticos.	<ul style="list-style-type: none"> • Contratos o instrumentos jurídicos.

1

(Handwritten marks)



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<ul style="list-style-type: none"> • 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 o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales; • 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; • Permitir a la SABG o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales; 		<p>Unidad administrativa encargada de la contratación de servicios informáticos.</p>	<ul style="list-style-type: none"> • Contratos o instrumentos jurídicos.

↓

9

2



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<ul style="list-style-type: none"> Colaborar con la SABG en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la LGPDPPS, proporcionando la 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. 			

Artículos vinculados: 57 y 58 de la LGPDPPSO.

5.U. TRANSFERENCIAS

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Formalizar las transferencias nacionales e internacionales mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, salvo en las siguientes excepciones:</p>	<ul style="list-style-type: none"> Identificar las transferencias que se realizan que requieren la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes. 	<ul style="list-style-type: none"> Todas las unidades administrativas que realicen transferencias. Unidad administrativa competente, en lo relativo a la elaboración y suscripción de las cláusulas contractuales, convenios de colaboración u otros instrumentos jurídicos. 	<ul style="list-style-type: none"> Cláusulas contractuales, convenios de colaboración u otros instrumentos jurídicos.

Handwritten marks: a stylized 'R' and a signature.

Handwritten number '1' in blue ink.



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<ul style="list-style-type: none"> • Cuando la transferencia sea nacional y se realice entre el sujeto obligado y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos. • Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el sujeto obligado y el responsable receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento que realiza el sujeto obligado. 	<ul style="list-style-type: none"> • Elaborar y suscribir las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, cuando se requiera. 		
<ul style="list-style-type: none"> • Sólo hacer transferencias fuera del territorio nacional cuando el tercero receptor se obligue a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las disposiciones que resulten 	<p>3. Para las transferencias y remisiones internacionales, previo a que éstas ocurran, se deberá solicitar al tercero receptor que <u>manifieste por escrito</u> que se obliga a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO y las</p>	<p>Todas las unidades administrativas que realicen transferencias.</p>	<ul style="list-style-type: none"> • Escritos de los terceros receptores de los datos personales.

1

g

z



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
aplicables en la materia.	disposiciones que resulten aplicables en la materia.		
<ul style="list-style-type: none"> Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen. 	<p>4. Cuando inicien las transferencias, comunicar el aviso de privacidad correspondiente. En lo sucesivo, sólo comunicar las modificaciones al aviso de privacidad original, cuando existan.</p>	Todas las unidades administrativas que realicen transferencias.	<ul style="list-style-type: none"> Evidencia de la comunicación del aviso de privacidad.
<p>Solicitar el consentimiento para las transferencias nacionales e internacionales, salvo en los siguientes casos:</p> <ul style="list-style-type: none"> Cuando la transferencia sea nacional y se realice entre el sujeto obligado y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos; Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México; Cuando la transferencia internacional se realice a petición de una autoridad extranjera u organismo internacional competente en su 	<p>5. Identificar las transferencias que requieren consentimiento de los titulares e informarlo en el aviso de privacidad.</p> <p>6. Solicitar el consentimiento de los titulares previo a la transferencia, cuando éste sea necesario y según la modalidad que se requiera (tácito o expreso y por escrito).</p>	Todas las unidades administrativas que realicen transferencias.	<ul style="list-style-type: none"> Consentimiento de los titulares.



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>carácter de receptor, siempre y cuando las facultades entre el sujeto obligado y el responsable receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento que realiza el sujeto obligado;</p> <ul style="list-style-type: none"> • Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; • Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia; • Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última; 		<p>Todas las unidades administrativas que realicen transferencias.</p>	<ul style="list-style-type: none"> • Consentimiento de los titulares.

1
9

2



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<ul style="list-style-type: none">• Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;• Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el sujeto obligado y el titular;• Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el sujeto obligado y un tercero;• Cuando se trate de los casos en los que el SAT no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 16 de la LGPDPSO; o• Cuando la transferencia sea necesaria por razones de seguridad nacional.			

T

1

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>En caso de que se requiera el consentimiento expreso, establecer el medio que permita obtenerlo de manera previa a la transferencia.</p> <p>Este medio deberá ser de fácil acceso y con la mayor cobertura posible, y considerar el perfil de los titulares y la forma en cómo se mantiene contacto cotidiano o común con ellos.</p>	<p>7. Establecer los medios para solicitar el consentimiento expreso, previo a la transferencia.</p>	<p>Todas las unidades administrativas que realicen transferencias.</p>	<ul style="list-style-type: none"> Medios establecidos para solicitar el consentimiento expreso, en caso de requerirse.
<p>Sólo tratar los datos que hayan sido transferidos al responsable para las finalidades para las cuales le hayan sido comunicados, según lo establecido en el aviso de privacidad proporcionado, así como garantizar la confidencialidad de los datos personales.</p>	<p>8. Implementar los controles de seguridad establecidos para la confidencialidad de los datos personales, y no tratar los datos personales para finalidades distintas.</p>	<p>Todas las unidades administrativas que realicen transferencias.</p>	<ul style="list-style-type: none"> Controles implementados.

Artículos vinculados: 60, 61, 62, 63, 64 y 65 de la LGPDPPSO.

A
D
Z



6.U. ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS ARCO

Los titulares de los datos personales tienen derecho a acceder a ellos, rectificarlos, a solicitar que se eliminen o cancelen, así como a oponerse a su uso. A estos derechos se les conoce como ARCO y están reconocidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

Al respecto, el Comité de Transparencia aprobó el Procedimiento Interno de Gestión de Solicitudes para el Ejercicio de Derechos ARCO y de Portabilidad³.

7.U. PORTABILIDAD

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Otorgar al titular una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos, cuando los mismos se traten en un formato con tales características, de conformidad con la LGPDPPSO y la normativa aplicable.	1. Atender las solicitudes del ejercicio del derecho de portabilidad según los criterios y parámetros establecidos por la LGPDPPSO.	Unidad de Transparencia y unidades administrativas responsables de atender las solicitudes de ejercicio de derechos ARCO.	Documentación que se genere para atender las solicitudes de portabilidad.

Artículos vinculados: 51 de la LGPDPPSO.

NOTA: Para cumplir con esta obligación, es necesario tener en cuenta lo que señala el artículo 51 de la LGPDPPSO, para la portabilidad de datos personales.⁴

³ Mediante la Quinta Sesión Extraordinaria del comité de Transparencia del Servicio de Administración Tributaria (CTSAT), de fecha 1 de abril de 2024

⁴ LGPDPPSO:

Artículo 51. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

6.2.4 Obligaciones relevantes en la etapa de ELIMINACIÓN de los datos personales

1.E. SUPRESIÓN DE LOS DATOS PERSONALES (CALIDAD)

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una vez que concluya su plazo de conservación establecido.	<ol style="list-style-type: none"> 1. Tener identificados los plazos de conservación de las series documentales que contienen datos personales. 2. Realizar la eliminación de los documentos correspondientes a dichas series documentales cuando haya concluido el plazo de conservación respectivo. 	Unidades administrativas competentes.	<ul style="list-style-type: none"> • Instrumentos de clasificación archivística. • Evidencia generada en la eliminación de los documentos. • Inventario de datos personales.
Previo a la supresión procederá el bloqueo.	<ol style="list-style-type: none"> 3. Considerar en el plazo de conservación y en el procedimiento de archivos, la etapa de bloqueo de los datos Personales. 	Unidades administrativas competentes.	<ul style="list-style-type: none"> • Procedimiento de archivo que incluye el bloqueo.
Establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.	<ol style="list-style-type: none"> 4. Establecer las políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, considerando los atributos de irreversibilidad; seguridad y confidencialidad, favorable al medio ambiente. 	Unidades administrativas competentes.	<ul style="list-style-type: none"> • Políticas, métodos y técnicas desarrolladas. • Documentación y evidencia que se genere con su implementación.

A
9
R



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>En las políticas, métodos y técnicas, se deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:</p> <p>I. Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales;</p> <p>II. Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la LGPDPPSO, y;</p> <p>III. Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.</p>		<p>Unidades administrativas competentes.</p>	<p>Políticas, métodos y técnicas desarrolladas.</p> <p>Documentación y evidencia que se genere con su implementación.</p>

Artículos vinculados: 17 de la LGPDPPSO

6.2.5 Otras Obligaciones

RESPONSABILIDAD			
Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Implementar las siguientes acciones para acreditar el cumplimiento de los principios, deberes y obligaciones, así como para rendir cuentas:</p> <ul style="list-style-type: none"> • Autorizar y destinar recursos para la instrumentación de programas y políticas de protección de datos personales. 	<p>1. Prever presupuesto para la instrumentación de programas y políticas de protección de datos personales.</p>	<p>Unidades administrativas competentes.</p>	<ul style="list-style-type: none"> • Presupuesto del ejercicio en curso.
<p>Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización, tomando en cuenta el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance, finalidades del tratamiento, atribuciones y facultades del responsable y demás cuestiones que se consideren convenientes.</p> <p>Para ello, el responsable podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas, o cualquier otro mecanismo que determine adecuado para tales fines.</p>	<p>2. Elaborar un programa de protección de datos personales que contemple el cumplimiento obligatorio al interior de la organización del responsable.</p>	<p>Comité de Transparencia.</p>	<ul style="list-style-type: none"> • Programa de Protección de Datos personales.

I
d

2



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.</p>	<p>3. Elaborar y aplicar un programa de capacitación y actualización de las personas servidoras públicas en materia de protección de datos personales, de conformidad con el apartado de Capacitación de este Programa.</p>	<ul style="list-style-type: none"> Comité de Transparencia. 	<ul style="list-style-type: none"> Programa de capacitación para personas servidoras públicas del sujeto obligado.
<ul style="list-style-type: none"> Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran. Establecer un sistema de supervisión y vigilancia interna y/o externas, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales. <p>Las revisiones de las políticas y programas de seguridad y del sistema de supervisión y vigilancia implementados se deberá realizar cada dos años, salvo que se realicen modificaciones sustanciales a los tratamientos y sea necesaria una revisión previa.</p>	<p>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.</p>	<ul style="list-style-type: none"> Comité de Transparencia. 	<ul style="list-style-type: none"> Programa de supervisión y vigilancia, y resultados obtenidos.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Establecer procedimientos para recibir y responder dudas y quejas de los titulares, que sea de fácil acceso y con la mayor cobertura posible; considerando la forma en que se mantiene contacto o comunicación directa o cotidiana con ellos, así como estar, en todo momento habilitado.</p>	<p>5. Establecer un procedimiento para atender dudas y quejas de los titulares con las características señaladas en la columna anterior.</p>	<p>Comité de Transparencia.</p>	<p>Procedimiento de Recepción Y Atención de Dudas y Quejas por Parte de las Personas Titulares de Datos Personales.</p>
<p>Diseñar, desarrollar e implementar las 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 LGPDPSO, y las demás que resulten aplicables en la materia, para lo cual se deberán aplicar las medidas de carácter administrativo, técnico, físico o cualquier otra que resulten necesarias.</p> <p>Para ello, se deberá considerar los avances tecnológicos, los costos de implementación, la naturaleza, el ámbito, el contexto y los fines del tratamiento de los datos personales, los riesgos de diversa probabilidad y gravedad que entraña éste para el derecho a la protección de datos</p>	<p>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.</p>	<p>Unidades administrativas competentes.</p>	<p>Políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.</p>

↓
g
r



Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>personales de los titulares, así como otros factores que considere relevantes el responsable.</p> <p>Garantizar que las 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 LGPDPSO y la normativa aplicable a la materia y que en particular que sean objeto de tratamiento los datos personales estrictamente necesarios para los fines del tratamiento, esto aplicará a la cantidad de datos personales recabados, al alcance del tratamiento, el plazo de conservación, entre otros factores relevantes.</p> <p>Para ello, se deberán implementar las medidas técnicas y organizativas apropiadas.</p>			
<p>Implementar mecanismos para evidenciar el cumplimiento de los principios, deberes y obligaciones ante los titulares y el SAT, tanto de tratamiento propios como de aquéllos realizados por los encargados y en las transferencias nacionales e internacionales.</p>	<p>7. En todos los casos generar pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPSO y demás disposiciones que resulten aplicables.</p>	<p>Unidades administrativas, Comité de Transparencia y Unidad de Transparencia.</p>	<p>Evidencia generada según lo establecido en la columna de "Medios para acreditar el cumplimiento" de todos los cuadros de este Programa.</p>

1

7

Artículos vinculados: 23 y 24 de la LGPDPPSO

EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
Realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el área establecida por la SABG cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas.	1. Documento mediante el cual se valoran 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 las personas titulares, así como los deberes de los responsables y las personas encargadas, previstos en las disposiciones jurídicas aplicables.	Comité de Transparencia.	<ul style="list-style-type: none"> Documento que se deberá presentar ante la SABG.
Atender el plazo para presentar la evaluación ante la SABG: 30 días anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología. Atender las observaciones que en su caso realice la SABG, y justificar cuando ello no sea posible.	2. Presentar en tiempo y forma las Evaluaciones que se requieran ante el área que establezca la SABG.	Comité de Transparencia y Unidad administrativa. Encargada de las políticas públicas, sistemas plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.	Documentación que se genere con motivo de la Presentación de la Evaluación ante la SABG y la atención de las observaciones que en su caso emita,

Artículos vinculados: 77 y 78 de la LGPDPPSO



FUNCIONES DEL COMITÉ DE TRANSPARENCIA

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales al interior del sujeto obligado, y al respecto, tendrá las siguientes funciones:</p> <ul style="list-style-type: none"> • Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales, de conformidad con las disposiciones previstas en la LGPDPPSO y en aquellas disposiciones que resulten aplicables en la materia; • Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes de los derechos ARCO; • Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO; • Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor 	<p>1. Establecer un programa de capacitación y actualización para las personas servidoras públicas, en materia de protección de datos personales.</p>	<p>Comité de Transparencia.</p>	<p>Programa de capacitación.</p>

1

T

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>observancia de la LGPDPSO y en aquellas disposiciones que resulten aplicables en la materia. Supervisar, en coordinación con las unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;</p> <ul style="list-style-type: none"> • Dar seguimiento y cumplimiento a las resoluciones emitidas por la SABG • Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales, y • Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen las unidades administrativas. 			

Artículos vinculados: 77 y 78 de la LGPDPSO

1
d
r



FUNCIONES DE LA UNIDAD DE TRANSPARENCIA

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>La Unidad de Transparencia tendrá las siguientes funciones en materia de protección de datos personales:</p> <ul style="list-style-type: none"> • Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales; • Gestionar las solicitudes para el ejercicio de los derechos ARCO; • Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados; • Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables; • Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO; • Aplicar instrumentos de evaluación de calidad sobre la 	<ol style="list-style-type: none"> 1. Establecer procedimientos internos para cumplir con sus funciones y para gestionar de manera eficiente las solicitudes de derechos ARCO. 2. Diseñar la metodología y programa de evaluaciones de calidad sobre la gestión de las solicitudes de ejercicio de los derechos ARCO, y aplicar dichas evaluaciones. 	<ul style="list-style-type: none"> • Unidad de Transparencia. 	<ul style="list-style-type: none"> • Procedimientos y programas establecidos e implementados.

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>gestión de las solicitudes para el ejercicio de los derechos ARCO, y</p> <ul style="list-style-type: none"> Asesorar a las unidades administrativas en materia de protección de datos personales. 			
<p>Auxiliar y orientar al titular en la elaboración de las solicitudes para el ejercicio de sus derechos ARCO, en todo momento, y en especial en aquellos casos en que el titular no sepa leer ni escribir, así como informar sobre la obligación del titular de acreditar su identidad y, en su caso, la identidad y personalidad de su representante.</p> <p>Para el caso de las personas con alguna discapacidad, la Unidad de Transparencia procurará atender a cada uno de los titulares, de acuerdo con su situación particular, facilitando en todo momento la información que éstos requieran para el ejercicio de sus derechos ARCO.</p>	<p>3. Auxiliar y orientar a los titulares en las presentaciones de sus solicitudes de ejercicio de derechos ARCO.</p>	<ul style="list-style-type: none"> Unidad de Transparencia. 	<ul style="list-style-type: none"> Procedimientos y programas establecidos e implementados.

Artículos vinculados: 79 y 80 de la LGPDPSO

↓

9

↓

CAPACITACIÓN

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios que facilitan la acreditación del cumplimiento
<p>Establecer un programa anual de capacitación y actualización en materia de protección de datos personales, dirigido tanto a personal como a encargados.</p> <p>El programa de capacitación deberá ser a corto, mediano y largo plazo y considerar los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de puesto.</p>	<p>1. Establecer un programa anual de capacitación y actualización en materia de protección de datos personales para las personas servidoras públicas y encargadas.</p>	<p>Comité de Transparencia con el área competente de recursos humanos o que lleve la capacitación del personal dentro del SAT.</p>	<p>Programa anual de capacitación.</p>

Artículos vinculados: 78 de la LGPDPPSO

El programa de capacitación deberá tomar en cuenta los siguientes niveles, para determinar el tipo de capacitación que requieren las personas servidoras públicas:

- a) **Concienciación:** programas a corto plazo para la difusión en general de la protección de datos personales en el SAT;
- b) **Entrenamiento:** programas a mediano plazo que buscan capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento de los datos personales, y
- c) **Educación:** programa general a largo plazo que tiene por objetivo incluir la protección de los datos personales dentro de la cultura de la organización.

Se debe realizar una detección de necesidades para identificar el nivel y tipo de capacitación necesaria para el personal, de acuerdo con las responsabilidades asignadas y tomando en cuenta su perfil de puesto, especialmente de aquéllos involucrados en el tratamiento de datos personales. Asimismo, se debe evaluar la eficiencia y eficacia de la capacitación, a través de criterios de evaluación que determinen el nivel de competencia aceptado por el sujeto obligado, y mantener un registro por cada persona servidora pública.



7. Sanciones por Incumplimiento

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar un exhorto a la unidad administrativa correspondiente para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 132 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, las siguientes:

Capítulo II

De las Sanciones

Artículo 132. *Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:*

- I. *Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;*
- II. *Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;*
- III. *Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;*
- IV. *Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;*
- V. *No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 21 de la LGPDPPSO, según sea el caso, y demás disposiciones que resulten aplicables en la materia;*
- VI. *Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;*
- VII. *Incumplir el deber de confidencialidad establecido en el artículo 36 de la LGPDPPSO;*
- VIII. *No establecer las medidas de seguridad en los términos que establecen los artículos 25, 26 y 27 de la LGPDPPSO;*
- IX. *Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 25, 26 y 27 de la LGPDPPSO;*
- X. *Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;*
- XI. *Obstruir los actos de verificación de la autoridad;*
- XII. *Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;*
- XIII. *No acatar las resoluciones emitidas por el Instituto, y*
- XIV. *Omitir la entrega del informe anual y demás informes a que se refiere el artículo 40, fracción VI de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.*



Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

I

d

X