Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Sector Público

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Directorio

Francisco Javier Acuña Llamas
Comisionado Presidente

Oscar Mauricio Guerra Ford
Comisionado

Blanca Lilia Ibarra Cadena
Comisionada

María Patricia Kurczyn Villalobos
Comisionada

Rosendoevgueni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

Joel Salas Suárez
Comisionado

Instituto Nacional de Transparencia, Acceso a la Información
y Protección de Datos Personales

Av. Insurgentes 3211, Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Ciudad de México, C.P. 04530

ÍNDICE

I. INTRODUCCIÓN

La presente publicación va dirigida a los Sujetos Obligados del ámbito federal en su carácter de responsables y obligados de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados *(en lo sucesivo Ley General)* [1] y los Lineamientos Generales de Protección de Datos Personales para el Sector Público *(en lo sucesivo Lineamientos Generales)*,[2] los Sujetos Obligados, que traten datos personales, deberán cumplir una serie de obligaciones con objeto de garantizar a las personas el derecho a la protección de su información personal.

La protección de datos personales es un derecho humano, reconocido en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos *(en lo sucesivo CPEUM)*, toda persona tiene derecho a la protección de sus datos personales, y se reconoce el derecho de acceso, rectificación y cancelación y oposición en los términos que las leyes establezcan.

En el año 2017 se promulgó la Ley General, con ello se fortaleció la reglamentación en materia de datos personales en el sector público, por lo que, tomando en consideración las atribuciones del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales *(en lo sucesivo INAI)* se crea y emite la presente guía, que pretende proporcionar apoyo técnico para el cumplimiento de la normatividad de la materia, con el objetivo de:

- Facilitar el cumplimiento de las obligaciones en materia de protección de datos personales, así como la implementación de las acciones que permitan alcanzar dicho cumplimiento;

- Ofrecer un material didáctico a los responsables del tratamiento, que les sirva de consulta y apoyo para el cumplimiento de los principios y los deberes que establece la norma;

- Proporcionar a los responsables del tratamiento un manual de auto-contenido que precise una serie de reglas claras y sencillas, con recomendaciones y consejos para la protección de los datos personales, que les permita mejorar el sistema de protección de los datos personales que están en posesión de los sujetos obligados;

- Desarrollar y proponer la adopción de criterios, estándares, recomendaciones y mejores prácticas en materia de protección datos personales, para el sector público.

[1] Publicada en el Diario Oficial de la Federación (en lo sucesivo DOF) el 26 de enero de 2017, disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

[2] Publicados en el DOF el 26 de enero de 2018, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

Se desarrolla la guía para cumplir con las obligaciones de quienes tratan datos personales en el sector público, en específico sobre los siguientes temas: principios, deberes, derechos ARCO, transferencias, las obligaciones de la relación responsable-encargado y el incumplimiento de obligaciones.

II. CONCEPTOS BÁSICOS PARA ENTENDER ESTA GUÍA

1. ¿Qué es el derecho a la protección de los datos personales?

Se trata de un derecho humano reconocido a nivel constitucional por los artículos 6 y 16, lo cuales imponen obligaciones a las personas físicas o morales del ámbito público y privado que tratan datos personales, y que reconoce derechos a los titulares de los datos, a fin de garantizar su privacidad, el buen uso de la información personal y el derecho a la autodeterminación informativa.

Por autodeterminación informativa se entiende el derecho de las personas para decidir, de manera libre e informada, sobre el uso de la información que les pertenece.

Todo tratamiento o uso de datos personales puede conllevar un riesgo si se da un mal uso, una inadecuada gestión o cuidado, tener como consecuencia una intromisión ilegítima en la privacidad y la autodeterminación informativa de la persona que es titular de los datos personales. En ese sentido, al tratar datos personales se adquieren obligaciones para garantizar su adecuado tratamiento.

Así pues, la Ley General tiene por objeto la protección de los datos personales en posesión de los Sujetos Obligados, con la finalidad de regular su tratamiento, a efecto de garantizar la protección de los datos, la privacidad y el derecho a la autodeterminación informativa de las personas.

Por sujetos obligados para efectos de la Ley General de la materia entendemos en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Tanto los Sindicatos, como las personas físicas o morales que reciben y ejercen recursos públicos o realicen actos de autoridad, quedan excluidos, al ser aplicables para estos últimos la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo LFPDPPP).

2. ¿Qué es un dato personal?

Es cualquier información concerniente a una persona física identificada o identificable, de manera enunciativa más no limitativa se consideran los siguientes: el nombre, los apellidos, la dirección postal, el número de teléfono, la dirección de correo electrónico, el número de pasaporte, una fotografía, la Clave Única de Registro de Población (CURP) o cualquier otra información que permita identificar al titular de los datos.
Se considera que una persona es identificable cuando su identidad puede determinarse mediante los datos personales de que se traten.

Es importante señalar que, si los datos personales son objeto de un procedimiento de disociación, es decir, no es posible asociarse a su titular, ni permitir su identificación. En estos casos dejaran de ser considerados como datos personales y por lo tanto no será aplicable la normatividad en la materia.

3. ¿Qué es un dato personal sensible?

Son aquellos datos personales que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para éste. Entre los datos personales sensibles encontramos los siguientes: origen racial o étnico; estado de salud (presente y futuro); información genética; creencias religiosas, filosóficas y morales; opiniones políticas y preferencia sexual.

4. ¿Qué se entiende por tratamiento de datos personales?

Tratar datos personales es un concepto amplio, que incluye: cualquier operación u operaciones realizadas mediante procedimientos manuales o automatizados, relacionados con las siguientes acciones:

Obtención	Utilización	Manejo
Uso	Comunicación	Aprovechamiento
Registro	Difusión	Divulgación
Organización	Almacenamiento	Transferencia
Conservación	Posesión	Disposición
Elaboración	Acceso	

Por ejemplo, un responsable del tratamiento puede obtener datos personales, a través de un formato de trámite, almacenarlos en el disco duro de una máquina o en la nube, utilizarlos para el cumplimiento de sus facultades y atribuciones, comunicarlos con el encargado que le brinda un servicio y suprimirlos cuando haya concluido la finalidad para la cual los obtuvo. Todas estas acciones se consideran tratamiento de datos personales.

5. ¿Quién es el titular de los datos personales?

Es la persona física a quien refieren y pertenecen los datos personales que son objeto de tratamiento. Por tanto, se consideran titulares de los datos, aunque éstos estén en posesión de un tercero para su tratamiento. Por ejemplo, el titular de los datos personales contenidos en un expediente laboral es el trabajador a quien refieren esos datos.

6. ¿Quién es el responsable del tratamiento?

Se entiende por responsable a quien **decide** sobre el tratamiento de los datos personales, es decir, quien establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión.

Para los efectos de la Ley General los responsables son los sujetos obligados siguientes: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos en el ámbito federal, estatal y municipal.

7. ¿Quién es el encargado del tratamiento?

Es la persona física o jurídica, pública o privada, ajena a la organización del responsable del tratamiento, que trata los datos personales a nombre y por cuenta del responsable. A diferencia de este último, el encargado no decide sobre el tratamiento de los datos personales, sino que lo realiza siguiendo las instrucciones del responsable. Por ejemplo: la expedición de credenciales institucionales, que realiza un encargado, los datos que le son remitidos solamente podrá usarlos con dicha finalidad.

Si el encargado tratara los datos personales para finalidades propias, de forma tal que decidiera sobre dicho tratamiento, se convertiría en un responsable, con todas sus obligaciones, y estaría sujeto a las sanciones previstas por la normativa correspondiente a particulares o sujetos obligados de acuerdo a la naturaleza del responsable, en caso de incumplimiento.

8. ¿A quién le aplica la Ley?

La Ley General aplica a TODOS los sujetos obligados en el ámbito federal, estatal y municipal, de observancia directa para los pertenecientes al orden federal: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que en el desarrollo de sus actividades traten datos personales, con la excepción de los siguientes supuestos:

1) Los sindicatos.
2) Cualquier otra persona física o moral que reciba y ejerza recursos públicos.
3) Cualquier otra persona física o moral que realice actos de autoridad en el ámbito federal, estatal y municipal.

En los tres responsables previamente antes señalados no aplicará la Ley General, serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

9. ¿Cuál es el objeto de la Ley General?

Establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados. Así como, establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales, y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, regular el debido tratamiento de los datos personales en posesión de los sujetos obligados.

La Ley General, así como la normatividad que de esta derive, cuando no indique lo contrario, aplica al tratamiento de datos personales que obren tanto en soporte físico, como electrónico, siempre y cuando las bases de datos en las que estén contenidos hagan posible el acceso a los datos con base en criterios determinados, como podrían ser criterios específicos de búsqueda, nombre de los titulares, fechas, tipo de tratamiento, orden alfabético, o cualquier otro. Lo importante es que se refiera a información concerniente a una persona física identificada o identificable.

10. ¿Cuál es el ámbito de aplicación territorial de la Ley?

La Ley General es de cumplimiento obligatorio en toda la República Mexicana y de aplicación directa para los sujetos obligados del orden federal, en su carácter de responsables.

11. ¿Qué es una transferencia de datos personales?

De conformidad con lo establecido en la Ley General transferencia es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

La comunicación puede producirse, entre otros actos, por el envío de los datos al tercero, por el hecho de mostrarlos en una pantalla o permitirle el acceso a los mismos.

La transferencia de datos personales puede ser nacional o internacional, según el destino de los datos personales. Este tipo de transferencias están reguladas de forma distinta, como se verá en la sección VIII de esta guía. No obstante, en ambos casos, es necesario que se cumpla con todos los principios y deberes de la protección de datos, que establece la Ley General y los Lineamientos Generales.

Ejemplos de transferencias:

- Una Secretaría de Estado o un organismo descentralizado (responsable del tratamiento) que comunica datos personales de sus trabajadores al Instituto

Mexicano del Seguro Social (tercero) o al Instituto de Seguridad y Servicios Sociales para los Trabajadores del Estado (tercero), en cumplimiento a sus obligaciones patronales.

- Un hospital público (responsable) proporciona información de un paciente a la aseguradora de este último (tercero), a fin de que aplique el seguro de gastos médicos.
- Una universidad pública (responsable) envía datos personales de sus alumnos que van a participar en un programa de intercambio a una universidad de otro país (tercero).

12. ¿Qué es una remisión de datos personales?

La remisión al igual que la transferencia supone una comunicación de datos personales. La diferencia entre ambos conceptos consiste en que, en este caso, dicha comunicación se produce **entre un responsable y un encargado** del tratamiento.

Las remisiones también pueden ser nacionales o internacionales. Sin embargo, ambas están reguladas de la misma forma (ver capítulo VII), pues sin importar que el responsable del tratamiento remita los datos personales a un encargado dentro o fuera del territorio nacional, el primero sigue siendo quien responde por el debido tratamiento de la información personal que comunicó.

Ejemplos de remisiones:

- Una Secretaría de Estado comunica datos personales a una empresa que le presta los servicios de elaboración de su nómina.
- Una institución financiera pública comunica datos personales a un despacho de cobranza para que le preste el servicio de cobranza extrajudicial.

* Una vez que hayan quedado claros estos conceptos, será más sencillo entender las siguientes secciones de esta guía. Le recomendamos consultar estas definiciones las veces que sea necesario a lo largo de la lectura de la guía.

III. DIAGNÓSTICO INICIAL: LO PRIMERO QUE DEBO HACER PARA CUMPLIR CON MIS OBLIGACIONES

La Ley General establece las bases, principios y procedimientos para garantizar el derecho de toda persona a la protección de sus datos personales, en posesión de los sujetos obligados. Y regular el tratamiento legítimo, controlado e informado de los datos personales, para garantizar así la privacidad de las personas y la protección de su información personal.

Este tratamiento legítimo, controlado e informado de los datos personales se basa en principios y deberes que los responsables deben observar en el tratamiento de los datos personales. En concreto, los principios y deberes se convierten en obligaciones concretas para el responsable, que tiene que cumplir, así como hacer cumplir, en cada una de las fases del tratamiento.

Para cumplir con estas obligaciones, en primer lugar, resulta importante que el responsable identifique sus procesos internos de cómo lleva a cabo el tratamiento de datos personales dentro de su organización. Para ello, es necesario que realice un diagnóstico que le permita identificar cuál es el flujo que, al interior de su organización y estructura, se sigue con respecto al tratamiento de los datos personales, desde que éstos se obtienen hasta que los mismos se eliminan.

En ese sentido, se debe considerar, al menos, lo siguiente:

- ¿De dónde se obtienen los datos personales? (a través del titular, transferencias, fuente de acceso público, etc.).
- Unidades administrativas de los sujetos obligados que recaban y/o tratan datos personales.
- En específico, qué servidores públicos, empleados o personas recaban y/o tratan datos personales.
- Las finalidades del tratamiento (para qué utiliza datos personales).
- En su caso, con quién y para qué se comparten datos personales (encargados o terceros).
- En dónde y cómo se almacenan los datos personales (lugar físico, como archiveros; o electrónico, como computadoras, servidores, entre otros).
- ¿Qué procedimientos, mecanismos y tecnología utilizan en el tratamiento?
- ¿Cuánto tiempo se conservan los datos personales?
- Procedimientos para la supresión, previo bloqueo de los de datos personales.

A continuación, y con base en lo anterior se incluye una lista de preguntas que le ayudarán a realizar el diagnóstico antes señalado:

1. ¿El responsable trata datos personales en el ejercicio de sus facultades cotidianas?

Los responsables en el marco de sus competencias y facultades para atender un trámite, para configurar una relación jurídica, en cumplimiento a una normatividad o cualquier otra actividad trata datos personales. Es importante recordar que un dato personal es cualquier información correspondiente a una persona física identificada o cuya identidad se pueda conocer a través de esa información, por ejemplo, nombre, apellidos, CURP, número de pasaporte, número de teléfono, dirección de correo electrónico, número de tarjeta de crédito, datos profesionales, laborales o académicos, salario, entre otros.

Si la respuesta a esta pregunta es SÍ, entonces el responsable debe cumplir con las obligaciones que establece la Ley General, según si es encargado o responsable.

2. ¿Qué calidad tiene conforme a la Ley General? ¿es responsable o encargado?

El responsable es cualquier sujeto obligado de acuerdo a la Ley General, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, que decide sobre el tratamiento de datos personales.

Un encargado es la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

La característica principal del responsable es que trata datos personales por cuenta propia, es decir, decide sobre los mismos, y el encargado solamente realiza las actividades que le son señaladas.

3. ¿Qué tipo de datos personales trata el responsable?

Se sugiere hacer un listado de TODOS los datos personales que se recaban y utilizan para las distintas actividades que realiza el responsable en el marco de sus facultades y atribuciones legalmente conferidas, debe hacerse la distinción de los datos personales sensibles.

4. ¿De dónde se obtienen los datos personales?

Los datos personales se pueden obtener de tres formas:

a) De forma personal.- Cuando el titular proporciona los datos personales al responsable o a la persona física designada por el responsable, con la presencia física de ambos. Por ejemplo, cuando el titular acude a un hospital público (responsable) y ahí mismo proporciona sus datos personales;

b) De manera directa.- Cuando el titular proporciona los datos personales por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, Internet o vía electrónica, entre otros.

Por ejemplo, cuando el titular envía sus datos por correo electrónico o cuando los comunica vía telefónica al responsable; o bien,

c) De manera indirecta.- Cuando el responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, como podría ser a través de transferencias o fuentes de acceso público.

Es importante identificar con claridad si los datos se obtienen directamente del titular, y si no es el caso, de qué fuente o transferencia concreta se están obteniendo, identificando con precisión el sitio de donde se recaban (por ejemplo, página de Internet, boletín, entre otros) o la persona física o moral que los comunica al Responsable.

Las fuentes de acceso público son aquellas bases de datos cuya consulta se pueda realizar por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación,

por ejemplo, los directorios telefónicos, el Diario Oficial de la Federación (en lo sucesivo DOF) o el Registro Nacional de Profesionistas de la Secretaría de Educación Pública.

5. ¿Qué persona, área o departamento del responsable trata los datos personales?

Por tratamiento se entiende la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

En ese sentido, se deberán identificar las personas, áreas, departamentos o direcciones de los sujetos obligados que realicen cualquiera de las actividades antes señaladas, así como identificar qué actividad en concreto realizan con los datos personales, por ejemplo, si los recaban y almacenan; si los recaban, transfieren o acceden a los mismos.

6. ¿Para qué fines se tratan los datos personales?

Es necesario identificar cada una de las finalidades concretas para las cuales se tratan los datos personales, lo cual se vincula de manera directa con las actividades en las cuales se utilizan datos personales, por ejemplo, nómina o expediente de personal, tramites o servicios que realizan las dependencias o sujetos obligados.

7. ¿Se comunican datos personales a encargados?

El responsable puede comunicar datos a los encargados, para que estos traten los datos a nombre y por cuenta del primero, a esta comunicación de datos personales se le denomina remisión. La relación entre ambos deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa aplicable.

El encargado puede ser una persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente trate datos personales, por ejemplo: una dependencia en su carácter de responsable, contrata a una persona jurídica para administrar la nómina de sus empleados.

8. ¿Se comunican datos personales a personas físicas o morales que no sean encargados? ¿A quién y para qué se comunican los datos?

Si, la comunicación de datos personales no solamente es con encargados, también puede ser el titular de los datos o con otro responsable. Por lo anterior, resulta necesario que el responsable identifique a quién se comunican los datos personales y para qué fines. Se recuerda que aquellas comunicaciones de datos personales a personas distintas al responsable, titular o encargado se les denomina **transferencias.**

9. ¿En dónde se almacenan los datos personales?

Los datos personales que trata pueden estar almacenados en soporte electrónico o físico.

10. ¿Por cuánto tiempo se conservan los datos personales?

Los plazos de conservación se atienden en cumplimiento a la legislación en materia de archivos. Los sujetos obligados deben considerar las disposiciones específicas para la conservación y destrucción de la información de la cual son Responsables.

Los sujetos obligados de conformidad con lo establecido en la Ley General de Archivos, deben determinar a través de un análisis de procesos y procedimientos: la vigencia de los documentos, plazos de conservación y el catálogo de disposición documental.[3]

11. ¿Cómo se suprimen los datos personales?

El procedimiento para la supresión de los datos personales se encuentra contenido en el artículo 23 de los Lineamientos Generales, que establece la obligación del responsable de establecer políticas, métodos y técnicas orientadas a la supresión de los datos:

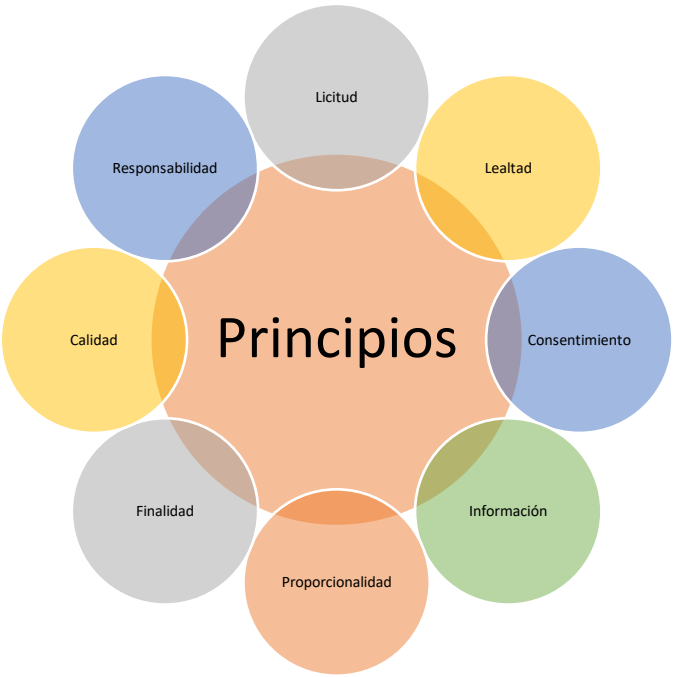
Estas políticas deben atender a los medios de almacenamiento ya sean físicos o electrónicos y deberán tener las siguientes características:

- Ser irreversible, el proceso utilizado no permite recuperar los datos.
- Ser seguro y confidencial, la eliminación debe atender a los deberes de confidencialidad y seguridad.
- Ser favorable al medioambiente, produzca la menor cantidad de emisiones y desperdicios.

[3] Para mayor información, se sugiere revisar el Título Tercero de la Valoración y Conservación de los Archivos, Capítulo I de la Valoración, de la Ley General de Archivos

IV. LOS PRINCIPIOS Y LAS OBLIGACIONES QUE CUMPLIR

El derecho a la protección de los datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones concretas para los responsables del tratamiento. Estos principios son los siguientes:



A continuación, se explican cada uno de estos principios, se identifican las obligaciones que se vinculan con los mismos y se dan sugerencias con relación a cómo cumplir con las mismas.

1. Principio de licitud

Los datos personales tienen que ser tratados por el responsable de manera lícita, lo que supone que el responsable debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga. En ese sentido, el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido, como cualquier acto de autoridad.

Dicho de otra forma, el principio de licitud significa que el tratamiento de datos personales es una actividad que depende de las atribuciones o facultades que previamente le otorga la ley a los Sujetos Obligados, en consecuencia, no deben tratarse datos personales si no se tienen facultades previamente otorgadas.

1.1 Obligaciones ligadas al principio de licitud:

De acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno al principio de licitud:

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

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

1.2 ¿Cómo cumplo con el principio de licitud?

Para la revisión sobre el cumplimiento del **principio de licitud** y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar la **página 17** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

2. Principio de lealtad

De acuerdo con el principio de lealtad, la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

- No se recaben datos personales con dolo, mala fe o negligencia;
- No tratar los datos de tal manera que genere discriminación o un trato injusto contra los titulares.
- No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado; y
- Se informen todas las finalidades del tratamiento en el aviso de privacidad.

Con este principio no se permite el tratamiento, tramposo, deshonesto y no ético de la información sobre los titulares, los derechos del titular dependen del Responsable, para que de esta manera el titular pueda confiar en la buena fe del Responsable por ello, es sancionable esa confianza depositada en el Responsable.

2.1 Obligaciones ligadas al principio de lealtad:

El responsable tiene las siguientes obligaciones en torno al principio de lealtad:

1) No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales.
2) Respetar en todo momento la expectativa razonable de privacidad del titular.

2.2 ¿Cómo cumplo con el principio de lealtad?

Para la revisión sobre el cumplimiento del **principio de lealtad** y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar las **páginas 18** y **19** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

3. Principio del consentimiento

Como regla general, el responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general. Por ejemplo:

> **Correcto:** solicitar el consentimiento para el envío de información relacionada con nuevos trámites sobre servicios que realiza el sujeto obligado.
>
> **Incorrecto:** solicitar el consentimiento para el uso de los datos personales en general, para cualquier finalidad que se le ocurra al responsable en el futuro. Por ejemplo: mencionar en el aviso de privacidad, sus datos personales serán recabados para las finalidades mencionadas y cualquier otra que se requiera.

El consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad (en el punto 4 de este apartado -Principio de información-, se explicará lo relativo al aviso de privacidad).

Además, el consentimiento debe ser libre tal y como lo refiere la Ley General, en el sentido que no medie error, mala fe, violencia o dolo que puedan afectar la voluntad del titular.

¿Cómo se obtiene el consentimiento?

El consentimiento puede ser tácito, expreso, o expreso y por escrito, dependiendo del tipo de datos personales que se tratarán, como se explica a continuación:

Tipo de consentimiento	¿Para qué tipo de datos personales se requiere?	¿Cómo se obtiene?
Tácito	Para cualquier tipo de dato personal, con excepción de los considerados como sensibles.	El consentimiento tácito se obtiene si el titular no se niega a que sus datos personales sean tratados, después de haber conocido el aviso de privacidad. Es decir, no es necesario que quede registrado que el titular autorizó el tratamiento de su información personal, sino que es suficiente con que no se niegue al tratamiento. Por ejemplo, el consentimiento tácito podría solicitarse a través de la siguiente frase: En caso de que no desee que sus datos personales sean tratados para las finalidades antes descritas, indíquelo a continuación; □ No consiento que mis datos personales sean tratados para las finalidades antes descritas. Si el titular no indicara en el recuadro que no consiente el tratamiento de sus datos personales, el responsable podría suponer que tiene el consentimiento para el tratamiento. Como es posible observar, no fue necesario que de manera expresa el titular indicara que consentía el tratamiento de su información personal, sino que fue suficiente con que no dijera que no
Expreso	Para cualquier tipo de dato personales, con excepción de los datos personales sensibles.	Este tipo de consentimiento deberá expresarse de las siguientes maneras: Verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología. Deberá implementarse un medio sencillo

		para manifestar la voluntad, por ejemplo: □ En caso de estar de acuerdo con recibir información, podrá manifestarlo señalando la casilla con X
Expreso y por escrito	Para datos personales sensibles.	El consentimiento se deberá otorgar por escrito, mediante firma autógrafa, huella dactilar, firma electrónica del titular o cualquier otro mecanismo autorizado que permita identificarlo plenamente, el cual podrá ser físico o electrónico. Por ejemplo: En caso de estar de acuerdo con las finalidades para las cuales se recaban sus datos personales sensibles, señale: _____ Nombre y Firma

Es importante tomar en cuenta que si una ley o reglamento, en lo particular, exige el consentimiento expreso o expreso y por escrito para el tratamiento, el responsable deberá solicitarlo de esa forma, aunque no se trate de datos sensibles. Por otra parte, si el responsable lo considera necesario o conveniente, o lo acuerda con el titular, podrá solicitar el consentimiento expreso, o expreso y por escrito, en cualquier caso. Lo importante es que el responsable tenga claro que cuando se trate de datos personales sensibles, el consentimiento deberá ser expreso y por escrito, cuando no se actualice alguno de los supuestos de excepción para recabar el consentimiento previstos en el artículo 22 de la Ley General.

¿Cómo se obtiene el consentimiento tácito de los titulares si no se recaben directamente del titular?

De acuerdo con lo señalado por el segundo párrafo del artículo 15 de los Lineamientos Generales, cuando el responsable no tenga contacto con los titulares previo a la utilización de sus datos personales, lo cual puede ocurrir cuando:

1. Los datos personales se obtengan de manera indirecta, es decir, cuando el titular no los haya proporcionado personalmente o de manera directa al responsable, como podría ser a través de una transferencia o fuente de acceso público, y
2. Se ponga a disposición del titular el aviso de privacidad por un medio que no permita el contacto personal o directo con éste, como por ejemplo su envío a través de correo postal.

El responsable podrá asumir que cuenta con el consentimiento tácito del titular para el tratamiento de sus datos personales, una vez que haya transcurrido cinco días hábiles, contados desde la fecha de envío del aviso de privacidad, y el titular no haya manifestado su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieren el consentimiento tácito.

Para ello, el responsable deberá informar en el aviso de privacidad que el titular cuenta con cinco días hábiles para manifestar su negativa para el tratamiento de su información para aquellas finalidades que requieren el consentimiento tácito.

Esta regla sólo aplica para el consentimiento tácito, cuando el responsable requiera el consentimiento expreso o expreso y por escrito, necesariamente tendrá que contactar personal o directamente al titular para obtenerlo, así como documentar la puesta a disposición del aviso de privacidad.

¿Cuándo se debe obtener el consentimiento?

El consentimiento se debe obtener en todos los casos, menos cuando ocurra alguno de los supuestos que prevé la Ley General en su artículo 22, los cuales son los siguientes:

- ✓ Cuando una ley así lo disponga, debiendo ser acorde a las bases, principios y disposiciones establecidos en la normatividad en materia de datos personales;
- ✓ Cuando las transferencias se realicen entre responsables, se trate de datos personales que utilicen en el ejercicio de las facultades del sujeto obligado o sean compatibles o análogas con la finalidad que dio origen al tratamiento de los datos personales;
- ✓ Cuando exista una orden judicial, resolución o mandato fundado y motivado de una autoridad competente;
- ✓ Para el reconocimiento o defensa de derechos del titular ante autoridad competente:
- ✓ Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- ✓ Cuando exista una situación de emergencia que pueda dañar a un individuo en su persona o sus bienes;
- ✓ Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;
- ✓ Cuando los datos personales figuren en fuentes de acceso público;
- ✓ Cuando los datos personales se sometan a un procedimiento previo de disociación, o
- ✓ Cuando el titular de los datos sea una persona reportada como desaparecida.

Entonces, cuando ocurra alguno de estos supuestos no será necesario la obtención del consentimiento, ni tácito, ni expreso, ni expreso y por escrito. Es importante señalar que una parte importante de los tratamientos ocurren en el marco de una relación jurídica entre el responsable y el titular, en la que no se requerirá el consentimiento.
Por relación jurídica se entiende el vínculo entre sujetos, respecto de determinados bienes o intereses, el cual está regulado por el derecho y tiene consecuencias jurídicas. Entonces, para determinar que una situación está enmarcada en una relación jurídica deben existir los siguientes factores:

- Un vínculo entre los sujetos;
- Dos o más sujetos;
- Estar regulado por el derecho, y
- Producir consecuencias jurídicas.

Es importante señalar que el hecho de que no se requiera el consentimiento para el tratamiento, no implica que no se deberán cumplir los otros principios, lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.

Con relación al tratamiento de **datos personales sensibles**, de acuerdo con el artículo 7 de la Ley General, no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley.

Ahora bien, si el tratamiento no actualiza alguna de las causales antes señaladas, el responsable requerirá el consentimiento del titular y éste se deberá pedir en los siguientes momentos:

Tipo de consentimiento	Si los datos se obtienen directamente del titular	Si los datos se obtienen de manera Indirecta
Tácito	Previo a la obtención de los datos personales.	Una vez que el responsable obtuvo los datos personales, deberá enviar al titular el aviso de privacidad correspondiente antes de que empiece a tratar los datos para las finalidades para las cuales los obtuvo. Si el aviso de privacidad se pone a disposición por un medio que permita el contacto directo con el titular (por ejemplo, teléfono o correo electrónico), el responsable podrá tratar los datos personales de manera inmediata, si después de que haya hecho del

		conocimiento del titular el aviso, éste no negó su consentimiento para el tratamiento de su información personal. Si el aviso de privacidad se pone a disposición por un medio que no permite el contacto directo con el titular (por ejemplo, por correo postal), el responsable deberá esperar cinco días, contados a partir del día siguiente de recibir el aviso de privacidad, para tratar los datos personales, en caso de que en dicho plazo no haya recibido la negativa del consentimiento por parte del titular.
Expreso	Previo a la obtención de los datos personales.	Una vez que el responsable obtuvo los datos personales, deberá enviar al titular el aviso de privacidad correspondiente antes de que empiece a tratar los datos para las finalidades para las cuales los obtuvo. En todos los casos, deberá esperar a obtener el consentimiento expreso del titular para tratar los datos personales.
Expreso y por escrito	Previo a la obtención de los datos personales.	Una vez que el responsable obtuvo los datos personales, deberá enviar al titular el aviso de privacidad correspondiente antes de que empiece a tratar los datos para las finalidades para las cuales los obtuvo. En todos los casos, deberá esperar a obtener el consentimiento expreso y por escrito del titular para tratar los datos personales.

¿Qué medios puedo utilizar para obtener el consentimiento expreso o expreso y por escrito?

El consentimiento expreso o expreso y por escrito se puede obtener a través del aviso de privacidad o de cualquier otro documento físico o electrónico que determine el responsable. En ese sentido, NO es necesario que el consentimiento se obtenga por medio del aviso de privacidad. Por ejemplo, el consentimiento expreso y por escrito se podría obtener a través

de un formato o contrato, y el expreso por medio de una grabación telefónica o de una casilla en formato electrónico. No obstante, hay que recordar que, en todos los casos, de manera previa se debe dar a conocer el aviso de privacidad.

Es importante tener en cuenta, que el medio que el responsable ponga a disposición del titular para obtener su consentimiento debe ser sencillo y gratuito.

¿Qué pasa si cambio las finalidades que originalmente informé en el aviso de privacidad?

Podría ser el caso de que el responsable decidiera tratar los datos personales para finalidades distintas a las que informó originalmente en el aviso de privacidad, y para las cuales obtuvo el consentimiento inicial por parte de los titulares.

En esos casos, será necesario solicitar el consentimiento de los titulares para las nuevas finalidades, siempre y cuando estas finalidades no actualicen los supuestos de excepción que señala el artículo 22 de la Ley General, antes mencionados.

Ahora bien, en estos casos en los que hubo cambio en las finalidades, será además necesario cumplir con el principio de información, que se explicará más adelante, de conformidad con lo siguiente:

- Si las nuevas finalidades requieren el consentimiento del titular, será necesario poner a su disposición un nuevo aviso de privacidad con la información relativa a las nuevas finalidades.
- Si las nuevas finalidades no requieren el consentimiento del titular, será suficiente con actualizar el aviso de privacidad existente e informar sobre estos cambios por el medio que así lo haya decidido el responsable y se haya incluido en el aviso de privacidad.

¿Cómo demuestro que cumplí con el principio del consentimiento?

Es importante señalar que quien está obligado a acreditar que obtuvo el consentimiento para el tratamiento de los datos personales, cuando éste se requiera, es el responsable. Para ello deberá generar las pruebas que considere pertinentes.

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

En el caso del consentimiento tácito, en virtud de que no hay una manifestación expresa del titular, las pruebas podrán ser aquéllas que permitan demostrar que el responsable puso a

disposición de los titulares el aviso de privacidad, por ejemplo, tener disponible el aviso de privacidad en las ventanillas donde se recaban los datos personales de los titulares o la constancia de correos electrónicos donde se envía el aviso de privacidad.

3.1 Obligaciones ligadas al principio de consentimiento:

El responsable tiene las siguientes obligaciones en torno al principio de consentimiento:

1. Obtener el consentimiento del titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos previstos en el artículo 22 de la Ley General;
2. Solicitar el consentimiento siempre ligado a finalidades específicas e informadas en el aviso de privacidad;
3. Determinar el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito;
4. Solicitar el consentimiento expreso y por escrito para los datos personales sensibles, en caso de que no se actualice alguno de los supuestos del artículo 22 de la Ley General;
5. Solicitar el consentimiento expreso o expreso y por escrito cuando así lo requiera una ley o reglamento, se acuerde con el titular o lo determine conveniente el responsable;
6. Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento;
7. Solicitar el consentimiento previo a la obtención de los datos personales, si éstos se recaban directamente del titular y no se actualiza alguno de los supuestos previstos en el artículo 22 de la Ley General;
8. Solicitar el consentimiento antes de utilizar los datos personales para las finalidades para las cuales se obtuvieron, si éstos se recabaron de manera indirecta y no se actualiza alguno de los supuestos previstos en el artículo 22 de la Ley General;
9. Implementar medios sencillos y gratuitos para la obtención del consentimiento, de acuerdo con el tipo de consentimiento que se requiera (tácito, expreso o expreso y por escrito);
10. Llevar un control para identificar a los titulares que negaron su consentimiento y a las finalidades concretas para las cuales no se podrán tratar los datos personales;
11. Esperar el plazo de cinco días hábiles que señala el artículo 15 de los Lineamientos Generales, para utilizar los datos personales, cuando éstos se hayan obtenido de manera indirecta, el aviso de privacidad se haya dado a conocer por un medio que no permita el contacto directo o personal con el titular y se requiera el consentimiento tácito;
12. Documentar su actuar para acreditar que se cumplió con el principio de consentimiento, y
13. Solicitar el consentimiento si hubo cambios en las finalidades informadas en el aviso de privacidad y éstas lo requieren por no actualizarse alguno de los supuestos previstos en el artículo 22 de la Ley General.

3.2 ¿Cómo cumplo con el principio de consentimiento?

Para la revisión sobre el cumplimiento del **principio de consentimiento** y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar las **páginas 23 a 37** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

4. Principio de información

Por virtud de este principio, los responsables se encuentran obligados a informar a los titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad. A fin de que los titulares puedan tomar decisiones informadas al respecto, y puedan ejercer su derecho a la protección de su información personal.

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

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad.

Asimismo, resulta pertinente aclarar que los responsables deben tener el número de avisos de privacidad que resulten necesarios de acuerdo con los tipos de tratamientos que realicen. Por ejemplo, se deberá elaborar un aviso de privacidad dirigido al personal del responsable y otro para los datos de los ciudadanos.

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

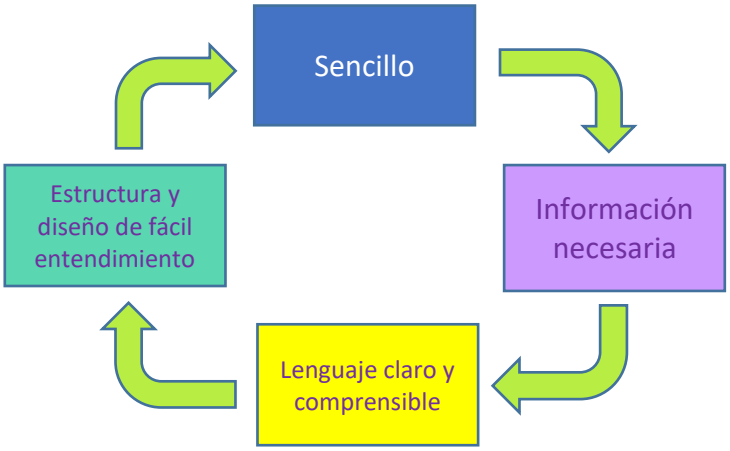
Con objeto de cumplir con esta obligación, el Instituto ha elaborado y puesto a disposición en su portal de Internet las siguientes herramientas:

1. El ABC del Aviso de Privacidad en el Sector Público; (en elaboración)
2. El formato de auto-evaluación de avisos de privacidad sector público, disponible en: http://inicio.ifai.org.mx/AvisoPrivacidad/AutoevaluacionResponsableSectorPublico1.docx

3. El Generador de Avisos de Privacidad (GAP) Sector Público, disponible en: http://gapsectorpublico.inai.org.mx/

En particular, se sugiere hacer uso del GAP, que es una herramienta informática gratuita, es una solución informática que ha sido desarrollada para facilitar la creación de avisos de privacidad que los responsables del tratamiento de datos personales, del sector público, tienen la obligación de poner a disposición de los titulares de los mismos, conforme a la normativa que les resulta aplicable.

¿Qué características debe tener un aviso de privacidad?



Lo anterior implica que en el aviso de privacidad se deberá:

- Abstener de usar frases inexactas, ambiguas o vagas;
- Tomar en cuenta el perfil de los titulares para su redacción;
- No incluir textos o formatos que induzcan al titular a elegir una opción en específico;
- No remitir al titular a textos y documentos que no estén disponibles; y
- No incluir casillas que estén marcadas previamente.

¿A través de qué medios puede difundirse o reproducirse el aviso de privacidad?

El aviso de privacidad podrá difundirse, ponerse a disposición o reproducir en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación.

En todo caso, el aviso de privacidad deberá estar ubicado en un lugar visible y que facilite su consulta. Esto último también tiene como finalidad acreditar ante el instituto el cumplimiento de su obligación.

Algunos ejemplos de medios para difundir el aviso de privacidad son los siguientes:

TIPO DE FORMATO	EJEMPLO
Físicos	Carteles o impresiones en papel
Electrónicos o digitales	En una página de Internet o pantallas Electrónicas
Ópticos o visuales	Videos o versión en caricatura
Sonoros	Grabación telefónica
Otro formato	Braille

¿Cuáles son las modalidades del aviso de privacidad?

De conformidad con la normatividad en materia de protección de datos personales, se reconocen dos modalidades: **integral y simplificado.**

¿Cuáles son los elementos del aviso de privacidad en cada una de las modalidades?

ELEMENTO INFORMATIVO	INTEGRAL	SIMPLIFICADO
1. Denominación del responsable.	➢	➢
1bis (opcional). Abreviatura o acrónimo por el cual se identifica al responsable.	➢	➢
2. Domicilio del responsable.	➢	
2bis (opcional). Datos de contacto.	➢	
3. Datos personales.	➢	
3bis (opcional). Medios y/o fuentes de obtención de los datos personales.	➢	
4. Finalidades del tratamiento.	➢	➢
5. Transferencias que requieren consentimiento	➢	➢
5bis (opcional). Transferencias que no requieren el consentimiento.	➢	
6. Negativa del consentimiento.	➢	➢
7. Sitio donde se podrá consultar el aviso de privacidad integral.		➢

8. Fundamento legal.	➢	
9. Derechos ARCO y Portabilidad.	➢	
10. Portabilidad	➢	
11. Domicilio de la Unidad de Transparencia.	➢	
12. Cambios al aviso de privacidad.	➢	
13. Fecha de elaboración o última actualización.	➢	➢
14. Características del aviso de privacidad	➢	➢

¿Cuándo puedo hacer uso de cada una de las modalidades de aviso de privacidad?

Dependiendo de la forma en que se obtengan los datos personales, puede determinarse el uso de las modalidades de los avisos de privacidad, tal y como se detalla a continuación:

Simplificado	El responsable deberá poner a disposición del titular el aviso de privacidad simplificado en un primer momento.
Integral	El aviso de privacidad integral deberá estar publicado, de manera permanente, en el sitio o medio que se informe en el aviso de privacidad simplificado.
	Nota: no implica que el aviso de privacidad integral no pueda ponerse a disposición del titular en un primer momento.

¿En qué momento se debe poner a disposición del titular el aviso de privacidad?

Por regla general, se deberá poner a disposición el aviso de privacidad previo al tratamiento de los datos personales. Por otro lado, es importante señalar que depende de la manera en la que se obtienen los datos, en qué momento se pone a disposición el aviso de privacidad, como se muestra a continuación:

Momento de la puesta a disposición	Forma de obtención de los datos personales
A. Previo a la obtención de los datos personales	**Personal**. Se entiende que los datos personales se obtienen de manera personal, cuando el titular los proporciona al responsable con la presencia física de

	ambos, por ejemplo, en una entrevista presencial o en las instalaciones del responsable. Directa. Por su parte, los datos personales se obtienen de manera directa cuando el propio titular los proporciona por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, Internet o vía telefónica. Por ejemplo, el llenado de un formulario por Internet, el envío de los datos personales por correo electrónico o la entrega de los datos personales a través de una llamada telefónica. En todos estos casos, el aviso de privacidad se debe dar a conocer previo a la obtención de los datos personales.
B. Al primer contacto con el titular	Indirecta. Se entiende que los datos personales se obtienen de manera indirecta cuando el responsable los obtiene sin que el titular se los haya proporcionado de forma personal o directa, como por ejemplo a través de una fuente de acceso público o una transferencia consentida por el titular o que no requiere su consentimiento. En estos casos en que el responsable no haya obtenido los datos personales directamente del titular, deberá dar a conocer el aviso de privacidad al primer contacto que tenga con éste, siempre y cuando el tratamiento requiera el contacto entre el responsable y el titular.
C. Previo al aprovechamiento de los datos personales	Datos obtenidos de manera indirecta. En estos casos, el responsable deberá dar a conocer su aviso de privacidad a los titulares, antes de que comience a utilizar los datos para las finalidades para las cuales se obtuvieron, partiendo del supuesto de que tiene datos de contacto de los titulares (para los casos en los que no se cuente con datos de contacto, ver apartado sobre medidas compensatorias de esta guía). Siguiendo el ejemplo anterior, el aviso de privacidad se debería dar a conocer antes de iniciar la elaboración del estudio.
D. Previo al aprovechamiento de los datos personales	Datos obtenidos previamente. Ahora bien, en este supuesto se parte del hecho de que el responsable ya tiene los datos personales del titular, los cuales obtuvo para cierta finalidad que le fue informada al titular en su momento, y que éste consintió, en el caso que se haya requerido el consentimiento. Sin embargo, el responsable requiere tratar los datos personales para nuevas finalidades. En un caso así, el

	responsable deberá poner a disposición del titular el aviso de privacidad con las nuevas finalidades, previo al aprovechamiento de los datos personales, es decir, antes de que los datos sean utilizados para las nuevas finalidades.

¿El responsable está obligado a demostrar la puesta a disposición del aviso de privacidad?

Los responsables están obligados a comprobar o demostrar que han puesto a disposición del titular el aviso de privacidad y que el mismo cumple con los requisitos que al efecto establece la Ley, su Reglamento y los Lineamientos, a través de los medios que estime pertinentes, como, por ejemplo, fotografías, grabaciones telefónicas, fe de hechos o firmas de los titulares, entre otros.

4.1 Obligaciones ligadas al principio de información:

El responsable tiene las siguientes obligaciones en torno al principio de información:

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

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

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

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

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

6. Redactar el aviso de privacidad de manera que sea claro, comprensible, con una estructura y diseño que facilite su entendimiento, para su elaboración tomar en cuenta el perfil de los titulares y atender lo siguiente: no usar frases inexactas, ambiguas o vagas; no

incluir textos o formatos que induzcan al titular a elegir una opción en específico; no pre-marcar casillas en las que se solicite el consentimiento del titular, y no remitir a textos o documentos que no estén disponibles;

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

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

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

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

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

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

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

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

15. Poner a disposición de los titulares un nuevo aviso de privacidad en los siguientes casos: (i) cambie la identidad del responsable; (ii) se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular; (iii) se requiera tratar los datos personales para nuevas finalidades que requieran el consentimiento del titular, y (iv) se requiera realizar nuevas transferencias que requieran el consentimiento del titular.

Una vez identificadas las obligaciones, en el siguiente apartado, se darán recomendaciones para cumplir con ellas.

4.2 ¿Cómo cumplo con el principio de información?

Para la revisión sobre el cumplimiento del principio de información y acceder a un listado de comprobación relacionado con este principio, se recomienda consultar el "ANEXO2-

PrincipiodeInformacion.docx" del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/AnexosDocumentoOrientador.zip

Para conocer más acerca de cómo cumplir con el principio de información y elaborar un aviso de privacidad, así como los medios y momentos para su puesta a disposición, se recomienda consultar y hacer uso de las siguientes herramientas:

La guía El ABC del Aviso de Privacidad en el Sector Público, disponible en el portal de Internet del INAI en ---------- y el Generador de Avisos de Privacidad disponible en el portal de Internet del INAI en:

http://gapsectorpublico.inai.org.mx/

Medidas compensatorias

Las medidas compensatorias son mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión en medios masivos de comunicación en lugar de hacerlo de manera personal o directa. Lo anterior, siempre y cuando resulte imposible dar a conocer el aviso de privacidad al titular de manera directa o exija esfuerzos desproporcionados.

Se considera que existe una imposibilidad para dar a conocer el aviso de privacidad de forma directa, cuando el responsable no cuente con los datos personales necesarios que le permitan tener contacto directo con los titulares, ya sea porque no existen en sus archivos, registros o bases de datos, o bien, porque los mismos se encuentran desactualizados, incorrectos, incompletos o inexactos.

¿Cuándo se considera que exige esfuerzos desproporcionados?

Cuando el número de titulares sea tal, que el hecho de poner a disposición de cada uno de éstos el aviso de privacidad de manera directa, le implique al responsable un costo excesivo atendiendo a su suficiencia presupuestaria, o comprometa la viabilidad de su presupuesto programado o la realización de sus funciones o atribuciones que la normatividad aplicable le confiera; o altere de manera significativa aquellas actividades que lleva a cabo cotidianamente en el ejercicio de sus funciones o atribuciones.

Ahora bien, para la implementación de medidas compensatorias, el responsable podrá realizarlo sin o con la autorización expresa del INAI, la cual se puede obtener a través de dos vías:

1. Actualizando los supuestos previstos en el ACUERDO mediante el cual se aprueban los criterios generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal, publicado en el DOF el 23 de enero de 2018, y
2. En caso de no actualizar estos supuestos, solicitando la autorización expresa del INAI.

¿En qué medios se deberán de publicarse los avisos de privacidad simplificados en la instrumentación de medidas compensatorias?

- DOF o diarios de circulación nacional;
- Diarios o gacetas oficiales de las entidades federativas, o diarios de circulación regional o local, o bien, revistas especializadas;
- Página de Internet o cualquier otra plataforma o tecnología oficial del responsable;
- Carteles informativos;
- Cápsulas informativas radiofónicas, o
- Cualquier otro medio alterno de comunicación masivo.

5. Principio de proporcionalidad

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

> √ **Correcto:** Cuando se realice un trámite concreto ante una dependencia de gobierno y el responsable solicite exclusivamente los datos personales que la legislación aplicable así lo manifiesta para el trámite correspondiente.
>
> X **Incorrecto:** Cuando se realice un trámite concreto ante una dependencia de gobierno y el mismo responsable solicite requisitos adicionales no estipulados en la normatividad y estos, contengan datos personales.

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

5.1 Obligaciones ligadas al principio de proporcionalidad:

En síntesis, de acuerdo con lo antes expuesto, el responsable tiene las siguientes obligaciones en torno al principio de proporcionalidad:

1. Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron;
2. Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles; y
3. Crear bases de datos con datos personales sensibles sólo cuando se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de la Ley General en la materia.

5.2 ¿Cómo cumplo con el principio de proporcionalidad?

Para la revisión sobre el cumplimiento del **principio de proporcionalidad** y acceder a un listado de comprobación relacionado con este principio, se recomienda revisar las **páginas 38 y 39** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

6. Principio de finalidad

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste. Las finalidades deben ser concretas, explicitas, licitas y legitimas:

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

La finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad. Un ejemplo de una finalidad es cuando un responsable, para contribuir a realizar un trámite solicitado por los titulares, señala que las finalidades del tratamiento de los datos personales que solicita son:

i) Creación de un expediente.
ii) Atención y seguimiento del trámite.
iii) Y generación de datos estadísticos entre los responsables.

En ese sentido, el responsable deberá evitar que las finalidades que describa en el aviso de privacidad sean inexactas, ambiguas o vagas, como “de manera enunciativa más no limitativa”, “entre otras finalidades”, “otros fines análogos”, “por ejemplo” o “entre otros”. Por ejemplo:

√ **Correcto:** Sus datos personales serán tratados con la finalidad de contribuir en la generación de información estadística en colaboración con el INEGI.
X **Incorrecto:** Sus datos personales serán tratados con la finalidad de contribuir en la generación de información estadística y otros fines análogos, en colaboración con el INEGI y demás instituciones.

Ahora bien, es necesario distinguir entre finalidades distintas a aquellas que motivaron su tratamiento original o que están previstas en el aviso de privacidad. Esto ocurre porque, de acuerdo con el artículo 10 de los Lineamientos Generales, el responsable deberá considerar 4 aspectos principales: La expectativa razonable de privacidad del titular basada en la relación que tiene con éste; la naturaleza de los datos personales; las consecuencias del tratamiento posterior de los datos personales para el titular; y las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y los Lineamientos Generales.

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

En ese sentido, se hace indispensable que en el aviso de privacidad se identifique y distinga las finalidades del tratamiento. Asimismo, se deberá indicar el mecanismo habilitado para que el titular, si así lo desea, pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades. Este mecanismo debe estar a disposición de los titulares previo a que su información personal sea tratada para dichos fines.

Ahora bien, como se explicó en el principio de consentimiento, cuando el aviso de privacidad no se haga del conocimiento del titular de manera personal o directa, por ejemplo, cuando se haga por envío postal, el aviso de privacidad debe indicar que el titular tiene un plazo de cinco días hábiles para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades que así lo considere.

¿Se pueden tratar los datos personales para finalidades distintas a las previstas en el aviso de privacidad?

El responsable solo podrá tatar datos personales que no hayan sido informados previamente al titular en los siguientes supuestos:

- Se cuente con atribuciones legales y medie el consentimiento del titular
- En términos de la Ley General
- Una persona reportada como desaparecida.

6.1 Obligaciones ligadas al principio de finalidad:

Derivado del cumplimiento al principio de finalidad el responsable tiene las siguientes obligaciones:

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

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

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

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

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

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

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

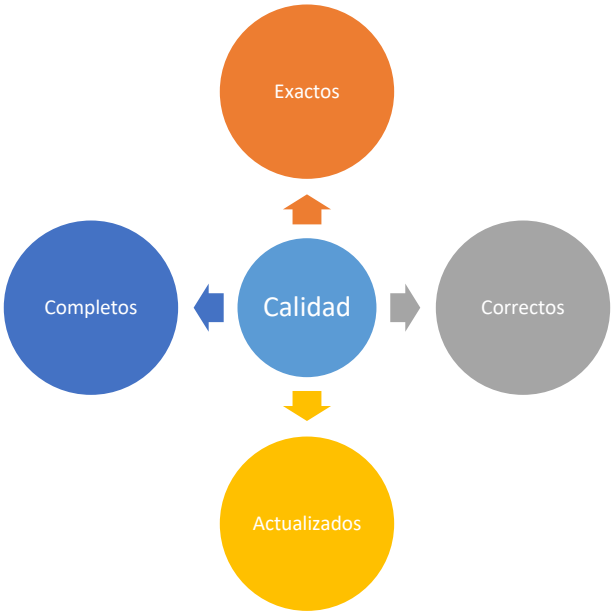
6.2 ¿Cómo cumplo con el principio de finalidad?

Para la revisión sobre el cumplimiento del **principio de finalidad** y acceder a un listado de comprobación relacionado con este principio, se recomienda revisar las **páginas 40 a 43** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

7. Principio de calidad

El principio de calidad significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser:



Los datos personales deben ser **exactos, correctos, completos y actualizados:**

- Los datos personales son **exactos y correctos** cuando en posesión del responsable no presentan errores que pudieran afectar su veracidad.

- Los datos personales son **completos** cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.

- Los datos personales están **actualizados** cuando los datos personales responden fielmente a la situación actual del titular.

El responsable debe adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con estas características, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

A efecto de cumplir con el principio de calidad, es necesario tomar en consideración los siguientes aspectos:

Datos obtenidos directamente del titular

- Se presume que los datos son exactos, completos, correctos y actualizados, hasta que manifieste o acredite lo contrario el titular.

Datos obtenidos indirectamente del titular

- Deberá el responsable adoptar las medidas necesarias para que los datos sean exactos, completos, actualizados y correctos.

¿Cuánto tiempo puedo conservar los datos personales?

El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con:

- Las disposiciones legales establecidas en la Ley General de Archivos;
- Las disposiciones aplicables en la materia de que se trate;
- Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y
- El periodo de bloqueo.

Ahora bien, es importante señalar que, en particular, el artículo 24 la Ley General, establece que se deben documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales respecto de cada tratamiento que se efectúe.

¿Qué se debe hacer cuando concluye el plazo de conservación?

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, el responsable debe proceder a la supresión de los datos personales. Es importante recordar que el plazo de conservación debe incluir un periodo de bloqueo, ya que los datos personales deben ser bloqueados antes de que sean eliminados o suprimidos.

Además, en cuanto a los **datos personales sensibles**, el responsable debe realizar esfuerzos razonables para **limitar el periodo** de tratamiento al mínimo indispensable.

El responsable debe establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

¿Qué significa el bloqueo de datos personales?

El bloqueo es la acción que tiene por objeto impedir el tratamiento de los datos personales para cualquier finalidad, con excepción de su almacenamiento y acceso para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, hasta el plazo de prescripción correspondiente. Concluido dicho periodo se deberá proceder a su supresión.

Por ejemplo, la secretaría -- tendría que bloquear los datos personales después de transcurrido los 15 años del tratamiento (10 años en que el titular tuvo una relación con esta + 5 años que establecía la norma). El tiempo en que los datos personales deberán estar bloqueados depende de los plazos legales que establezca la legislación de índole archivística para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, lo cual dependerá, a su vez, de la materia de que se trate. Concluido el periodo de bloqueo, el responsable deberá suprimir los datos personales.

7.1 Obligaciones ligadas al principio de calidad:

El responsable tiene las siguientes obligaciones en torno al principio de calidad:

- Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación;
- Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;
- Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales;
- Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley General de Archivos;
- Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.
- En caso de que se requiera, demostrar que los datos personales se conservan, bloquean y suprimen cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación.

7.2 ¿Cómo cumplo con el principio de calidad?

Para la revisión sobre el cumplimiento del **principio de calidad** y acceder a un listado de comprobación relacionado con este principio, se recomienda revisar las **páginas 43 a 45** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

8. Principio de responsabilidad

El principio de responsabilidad cierra el círculo con relación a los principios que regulan la protección de los datos personales. A este principio establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y los órganos garantes, que cumple con sus obligaciones en torno a la protección de los datos personales.

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

Para cumplir con el principio de responsabilidad, el responsable puede hacer uso de:

- Estándares
- Mejores prácticas nacionales e internacionales

Por ejemplo, el responsable podría una política interna dentro de su programa de protección de datos personales, dirigida a quienes traten datos bajo su supervisión o por su cuenta, que incluya medidas y controles que sirvan para garantizar el cumplimiento de la normatividad.

¿Qué mecanismos se pueden adoptar para cumplir con el principio de responsabilidad?

Se debe tomar en cuenta que los mecanismos que adopte el responsable, además de garantizar el debido tratamiento, deben privilegiar los intereses del titular y su expectativa razonable de privacidad.

Ahora bien, existen mecanismos que el responsable debe adoptar, los cuales se encuentran señalados en el artículo 30 de la Ley General que establece lo siguiente:

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

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

8.1 Obligaciones ligadas al principio de responsabilidad

El responsable tiene las siguientes obligaciones en torno al principio de responsabilidad:

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

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

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

8.2 ¿Cómo cumplo con el principio de responsabilidad?

Para la revisión sobre el cumplimiento del **principio de responsabilidad** y acceder a un listado de comprobación relacionado con este principio, se recomienda revisar las **páginas 69 a 73** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

V. LOS DEBERES Y LAS OBLIGACIONES QUE CUMPLIR

La protección de los datos personales además de principios y obligaciones encuentra su base en dos deberes: el de confidencialidad y el de seguridad.

A. Deber de Confidencialidad

De conformidad con los estándares internacionales por confidencialidad se entiende que el responsable debe establecer controles o mecanismos que tengan por objeto que todas aquellas personas que traten datos personales, en cualquier fase del tratamiento mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma.

Implica la obligación de guardar secreto respecto de los datos personales que son tratados, para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

Cuando se tratan datos personales, el responsable tiene que adoptar medidas para evitar que quienes tengan acceso a éstos, divulguen dicha información. Incluso la obligación de confidencialidad tiene que hacerse cumplir una vez que finalice la relación jurídica, a través de cláusulas de confidencialidad establecidas en los instrumentos jurídicos suscritos entre el responsable del tratamiento y quien tenga acceso a los datos personales.

B. Deber de Seguridad

Un pilar básico para una efectiva protección de los datos personales es la implementación de un Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), que permita planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico, a través de una serie de actividades interrelacionadas y documentadas tomando en consideración los estándares nacionales e internacionales, en materia de protección de datos personales y seguridad.

¿Qué es el Sistema de Gestión de Seguridad de Datos Personales?

Así como el Aviso de Privacidad es la materialización del principio de información, el Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión) es la materialización de los deberes de seguridad y confidencialidad.

Por Sistema de Gestión de Seguridad de los Datos Personales se entenderá al conjunto de elementos y actividades relacionadas entre sí, que le permitirán al responsable planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico, tomando en consideración la normatividad aplicable, así como los estándares a nivel nacional e internacional, en materia de protección de datos personales y seguridad.

La seguridad de la información debe preservar la confidencialidad, integridad y disponibilidad de los datos personales, por estos términos entendemos lo siguiente:

- Integridad: es la propiedad de salvaguardar la exactitud y completitud de la información, así como evitar la modificación no autorizada o accidental de la misma.
- Confidencialidad: es la propiedad de la información para no estar a disposición o ser revelada a personas no autorizadas.
- Disponibilidad: es la propiedad de un dato para ser accesible y utilizable, prevenir interrupciones no autorizadas.

Para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), se debe hacer basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar). Así como también, de estas actividades interrelacionadas para la protección de los datos personales. El responsable debe implementar un sistema de gestión contemplando cuando menos los siguientes aspectos:

a) Crear políticas internas para la gestión y tratamiento de los datos personales;
b) Elaborar un inventario de datos personales;
c) Definir funciones y obligaciones del personal que trate datos personales;
d) Realizar un análisis de riesgo de los datos personales, el cual deberá considerar amenazas, vulnerabilidades existentes y recursos involucrados en el tratamiento;

e) Realizar un análisis de brecha. (consistente en comparar las medidas de seguridad existentes contra las medidas de seguridad faltantes;
f) Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes y el cumplimiento cotidiano de sus políticas de gestión;
g) Monitorear y revisar de manera periódica las medidas de seguridad implementadas; y
h) Diseñar y capacitar al personal del responsable.

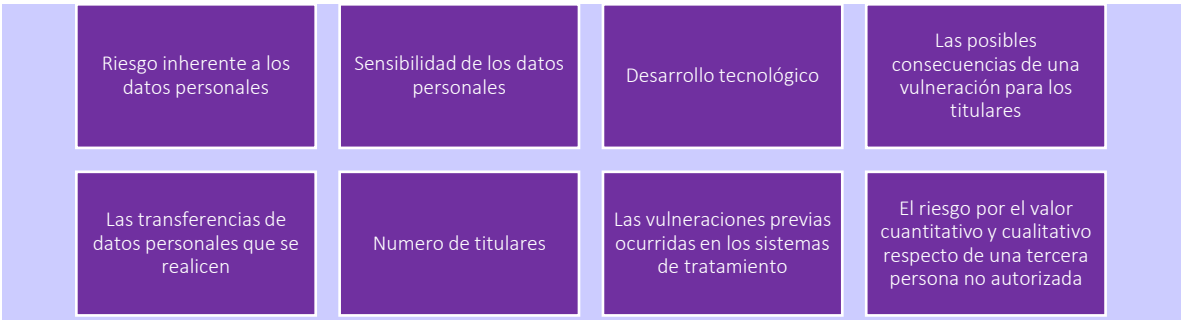
Visto lo anterior, el SGSDP funciona a través de un ciclo de mejora continua, dividido en 4 fases que consideran 9 pasos o actividades para la seguridad de los datos personales:

Fase 1. Planear el SGSDP	Paso 1. Establecer el Alcance y Objetivos	Paso 2. Elaborar una Política de Gestión de Datos Personales	Paso 3. Establecer Funciones y Obligaciones
	Paso 4. Elaborar un Inventario de Datos Personales	Paso 5. Realizar un Análisis de Riesgo de Datos Personales	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha
Fase 2. Implementar el SGSDP	Paso 7. Implementación de las Medidas de Seguridad aplicables a los Datos Personales		
Fase 3. Monitorear y Revisar el SGSDP	Paso 8. Revisiones y Auditoria		
Fase 4. Mejorar el SGSDP	Paso 9. Mejora Continua		

La implementación de estas actividades debe realizarse de manera coordinada, teniendo como objetivo principal identificar los riesgos y gestionar la seguridad de los datos personales a efecto de minimizar las vulneraciones a los mismos.

¿Qué factores se deben tomar en cuenta para determinar las medidas de seguridad?

Las medidas de seguridad son el conjunto de acciones y actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales. Para determinar qué medidas de seguridad se deben implementar, el responsable deberá tomar en cuenta los siguientes factores:



¿Cómo implementar las acciones para la seguridad de los datos personales?

A través de los siguientes mecanismos:

a) Políticas internas para la gestión y tratamiento de los datos personales

Para crear políticas internas referentes a la gestión y tratamiento de los datos personales, se deben observar los artículos 47 y 56 de los Lineamientos Generales, en primer término se deben elaborar e implementar políticas y programas de protección de datos personales, cuyo objeto sea establecer las directrices, la operación y el control de los procesos de tratamiento de datos realizado en ejercicio de sus atribuciones y funciones, a efecto de proteger los datos personales de una manera sistemática y continua.

El Comité de Transparencia, deberá aprobar, coordinar y supervisar las políticas y el programa de protección de datos del responsable, éste a su vez deberá destinar recursos de conformidad con la normatividad que le resulte aplicable para la implementación y cumplimiento de dicho programa y las políticas.

Entre los puntos que deben contener las políticas internas de gestión y tratamiento de los datos personales están las siguientes:

- Cumplimiento de todos los principios, deberes, derechos y obligaciones.
- Responsabilidades específicas de los involucrados en el tratamiento de los datos.
- Sanciones en caso de incumplimiento.
- Identificar el ciclo de vida de los datos personales, esto debe realizarse de conformidad con la Ley General de Archivos y la normatividad aplicable a cada sujeto obligado, para lo cual deberá contar con su catálogo de disposición documental.
- El proceso para el establecimiento de los mecanismos y medidas de seguridad.
- La atención de las solicitudes para el ejercicio de derechos ARCO.

Cabe destacar que las políticas internas para la gestión de los datos personales deben establecer el compromiso de cumplir con la legislación en la materia, por parte de todos los involucrados en el tratamiento a su vez que ésta debe ser comunicada.

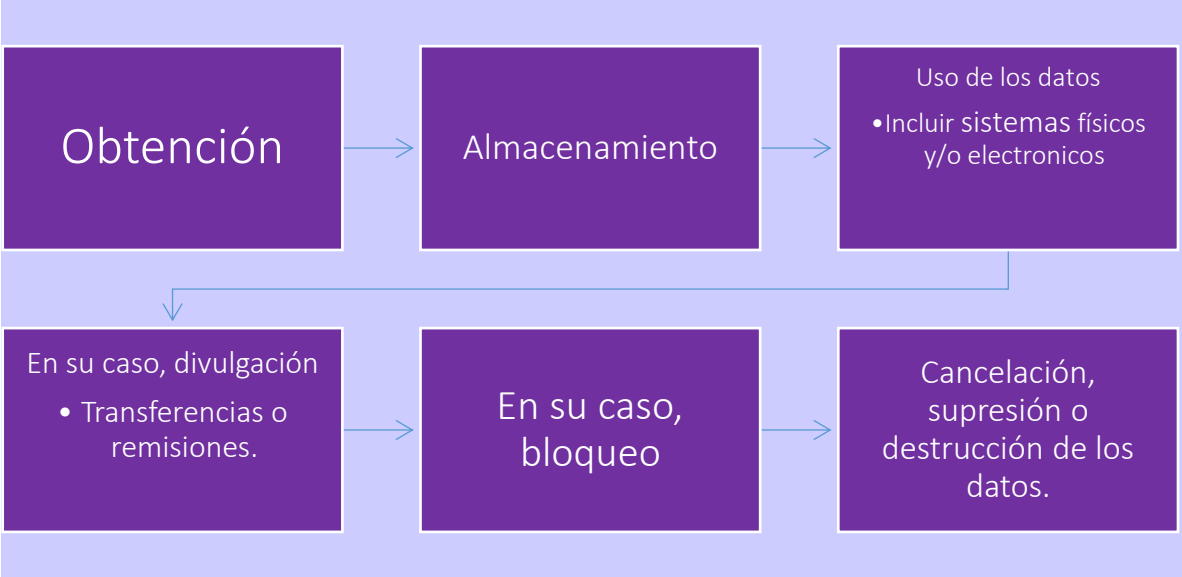
b) El inventario de datos personales y de los sistemas de tratamiento

Es necesario elaborar un inventario[4] con la información de cada tratamiento de datos que realice el responsable, que contenga un catálogo de medios físicos y electrónicos, finalidades, tipo de datos tratados, formatos de almacenamiento, lista de los servidores

[4] Artículos 58 y 59 de los Lineamientos Generales

públicos que tienen acceso al tratamiento, en su caso, nombre o razón social del encargado, así como de los destinarios de las transferencias.

También deberá considerar el ciclo de vida de los datos personales conforme a lo siguiente:



En efecto, realizar el inventario de datos personales implica llevar a cabo un diagnóstico de los datos personales y sistemas de tratamiento que se encuentran bajo resguardo del sujeto obligado, identificando los siguientes elementos relevantes:

1. Cada uno de los procesos en los que la unidad administrativa trata datos personales.
2. La unidad administrativa que está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.
3. De acuerdo con el ciclo de vida de los datos personales, se debe identificar:

    I. ¿Cómo se obtienen los datos personales?
    II. ¿Qué tipo de datos personales se tratan? ¿Son sensibles?
    III. ¿Dónde se almacenan los datos personales?
    IV. ¿Para qué finalidades se utilizan los datos personales?
    V. ¿Quién tiene acceso a la base de datos o archivos y a quién se comunican los datos personales al interior de la organización?
    VI. ¿Intervienen encargados en el tratamiento de los datos personales?
    VII. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
    VIII. ¿Se difunden los datos personales?
    IX. ¿Cuál es el plazo de conservación de los datos personales?

En este contexto, el documento que puede ser de utilidad, lo es el inventario de datos contenido en el Anexo I, del documento orientador el cual podrá descargar y utilizar en el siguiente hipervínculo:

http://inicio.ifai.org.mx/DocumentosdeInteres/AnexosDocumentoOrientador.zip

descargados los archivos corresponde al Excel denominado "ANEXO1-InventariodeTratamientos.xlsm"

c) Las funciones y obligaciones de las personas que traten datos personales

Para definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales, se debe atender lo que establece el artículo 57 de Los Lineamientos Generales, que estipula que se deberán establecer y documentar los roles y responsabilidades para todos aquellos que intervienen en el tratamiento de los datos personales dentro de la organización del sujeto obligado.

Además, se debe contar con mecanismos para asegurar que todas las personas involucradas en el tratamiento conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, y las consecuencias en caso de incumplimiento.

d) El análisis de riesgos

Para realizar un análisis de riesgo, se deben identificar escenarios de riesgo, tomando en consideración las amenazas y vulnerabilidades existentes para los datos personales. Asimismo, el artículo 32 de la Ley General establece una serie de medidas de seguridad que debe considerar el responsable para su implementación, que por su importancia se transcriben:

> *"Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:*
>
> *I. El riesgo inherente a los datos personales tratados;*
> *II. La sensibilidad de los datos personales tratados;*
> *III. El desarrollo tecnológico;*
> *IV. Las posibles consecuencias de una vulneración para los titulares;*
> *V. Las transferencias de datos personales que se realicen;*
> *VI. El número de titulares;*
> *VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y*
> *VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión."*

Respecto del análisis de riesgo, su cumplimiento se debe realizar considerando lo establecido en los Lineamientos Generales5 que establecen lo siguiente:

- Requerimientos regulatorios, códigos de conducta o mejores prácticas para los diferentes sectores.
- Definir el ciclo de vida y el valor de los datos personales.
- La exposición de los activos involucrados en el tratamiento de los datos.
- Las consecuencias en caso de una vulneración de seguridad.

De manera que, el análisis de riesgo implica que el sujeto obligado plantee directrices para tratar el riesgo, considerando los factores citados anteriormente, en función del alcance y objetivos del Sistema de Gestión. Esta actividad incluye realizar una ponderación de los escenarios de riesgo identificados a través de los siguientes pasos:

- Identificar activos
- Identificar amenazas
- Identificar vulnerabilidades

Como sugerencia podrá utilizar el evaluador de vulneración del INAI, el cual es una herramienta que permite a los responsables en materia de la Ley General revisar los posibles riesgos en los tratamientos que realizan a través de una serie de preguntas cerradas.

Esta herramienta permite generar múltiples evaluaciones para el sujeto obligado, así mismo es una herramienta desarrollada exclusivamente para apoyar y orientar en el cumplimiento de la normativa en materia de protección de datos personales, por lo que no exime a los responsables y sujetos obligados de realizar las acciones que resulten complementarias y necesarias para cumplir de manera integral con sus obligaciones normativas en la materia.

Para conocer y descargar estar herramienta podrá realizarlo desde el portal de internet del INAI, en el siguiente hipervínculo:

http://inicio.ifai.org.mx/SitePages/Evaluador-Vulneraciones.aspx

e) El análisis de brecha

Es importante que los sujetos obligados en su carácter de responsables, establezcan y mantengan medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos, protegiendo los mismos contra daño, perdida, alteración, destrucción o una utilización no autorizada de los mismos.

[5] Artículo 60 de los Lineamientos Generales.

Como se dijo anteriormente, la Ley General define las medidas de seguridad como el conjunto de acciones y actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales; cada una de estas medidas de seguridad se definen legalmente de la siguiente manera:

Las **medidas de seguridad administrativas**[6] 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**[7] son el 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: **a)** Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; **b)** Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; **c)** Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y **d)** Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.	Asimismo, las medidas de **seguridad técnicas**[8] 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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: **a)** Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; **b)** Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; **c)** Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y **d)** Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Ahora bien, por lo que hace al análisis de brecha, los Lineamientos Generales[9] contemplan que debe considerarse lo siguiente:

[6] Artículo 3, fracción XXI de la Ley General
[7] Artículo 3, fracción XXII de la Ley General
[8] Artículo 3, fracción XXIII de la Ley General
[9] Artículo 61 de los Lineamientos Generales

- Medidas de seguridad existentes y efectivas
- Medidas de seguridad faltante
- La existencia de nuevas medidas de seguridad que pudieran remplazar a las actuales.

Visto lo anterior, cabe destacar que el análisis de brecha se refiere al proceso de evaluación de las medidas de seguridad administrativas, físicas y técnicas, existentes y las que operan correctamente en la organización, contra las que serían necesarias tener para mitigar los riesgos de seguridad identificados en el análisis previo, así como las nuevas medidas de seguridad que podrían reemplazar a uno o más controles implementados actualmente.

f) El plan de trabajo

Una vez realizados los análisis correspondientes entre los que se encuentran los de riesgos y de brecha, se debe elaborar un plan de trabajo con la finalidad de implementar las medidas de seguridad faltantes, así como para el cumplimiento cotidiano de las políticas de tratamiento de los datos personales.

Para ello, se deben priorizar las medidas de seguridad más relevantes e inmediatas a establecer, habrá de considerarse los recursos económicos y humanos con los que cuenta el responsable para el cumplimiento, como todo plan de trabajo es indispensable que se fijen fechas compromiso, personas a cargo de su cumplimiento y para su implementación.

g) Los mecanismos de monitoreo y revisión de las medidas de seguridad

Como parte de la evaluación de las políticas implementadas en materia de seguridad y tratamiento de los datos personales, debe monitorearse y revisarse las medidas de seguridad, al respecto los Lineamientos Generales[10] establecen que debe supervisarse lo siguiente:

- Nuevos activos gestionados;
- Modificaciones necesarias;
- Nuevas amenazas dentro o fuera de la organización;
- Posibilidad de nuevas vulneraciones, por las amenazas correspondientes;
- Vulneraciones identificadas para determinar amenazas nuevas;
- Impacto de amenazas valoradas, vulnerabilidades y riesgos en conjunto;
- Incidentes y vulneraciones de seguridad ocurridas.

De conformidad con la Ley General se consideran como vulneraciones de seguridad las siguientes:

[10] Artículo 63 de los Lineamientos Generales

La perdida o destrucción no autorizada

El robo, extravio o copia no autorizada

El uso, acceso o tratamiento no autorizado

El daño, la alteración o modificación no autorizada

Dicho lo anterior, el monitoreo y revisión de las medidas de seguridad es el proceso de supervisar el funcionamiento del sistema de gestión y evaluar los objetivos, políticas, procesos y procedimientos establecidos en el mismo, con el fin de cumplir con la legislación en protección de datos personales.

De igual forma, para llevar a cabo dicha revisión de manera efectiva, es necesario monitorear continuamente los eventos que señala el artículo 63 de los Lineamientos Generales.

De tal manera que, cuando el sujeto obligado sufra alguna vulneración a la seguridad, éste deberá actuar conforme a lo dispuesto en los artículos 37, 38, 39, 40 y 41 de la Ley General. Asimismo, para el caso de las notificaciones sobre vulneraciones, deberá observar los artículos 66, 67 y 68 de los Lineamientos Generales.

Para conocer mayor información sobre vulneraciones usted puede consultar las Recomendaciones para el manejo de incidentes de seguridad de datos personales, documento que tiene por objeto describir los procesos y controles recomendados por el Instituto para generar un plan de respuesta a incidentes de seguridad, en particular para mitigar las vulneraciones a la seguridad de los datos personales, el cual se encuentra disponible en el siguiente hipervínculo:

http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

h) El programa general de capacitación

Como parte de las actividades interrelacionadas también se encuentra la capacitación, el diseñar e implementar programas a corto, mediano y largo plazo, para los involucrados en el tratamiento de los datos personales, atendiendo a sus roles, funciones y responsabilidades asignados.

Por lo tanto, a fin de contar con personal consciente de sus responsabilidades y deberes respecto de la protección de datos personales, se deben establecer y mantener programas de capacitación considerando las siguientes etapas:

1. **Concienciación:** programas a corto plazo para la difusión en general de la protección de datos personales en la organización.
2. **Entrenamiento:** programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidades en el tratamiento y seguridad de los datos personales.
3. **Educación:** programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de la organización.

Documento de seguridad

Por documento de seguridad entendemos que es el 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.

Este documento de manera particular deberá contener lo siguiente:

- Inventario de datos personales;
- Funciones de las personas que tratan datos;
- Análisis de riesgos;
- Análisis de brecha;
- Plan de Trabajo;
- Mecanismos de monitoreo y revisión;
- Programa de Capacitación.

Derivado de lo anterior, el contenido del documento de seguridad se integra por una serie de acciones que debe realizar el sujeto obligado para garantizar la seguridad de los datos personales, mismas que ya se señalaron como parte del Sistema de Gestión.

En este sentido, conforme se documenten las actividades que integran dicho Sistema de Gestión, el responsable deberá tomar en cuenta los eventos señalados por el artículo 36 de la Ley General para la debida actualización del Documento de Seguridad.

Finalmente, es importante destacar que la seguridad de los datos personales debe observarse durante todo su ciclo de vida, desde su obtención hasta su eliminación.

¿Con qué frecuencia debo realizar actualizaciones al documento de seguridad?

El documento deberá actualizarse cuando ocurran los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales, que impliquen un cambio en el nivel de riesgo;
- Atendiendo a una mejora continua, por el monitoreo y revisión del sistema de gestión;
- Por un proceso de mejora, para disminuir el impacto de una vulneración a la seguridad;
- Como parte de las acciones preventivas y correctivas de una vulneración.

¿Qué hacer en caso de una vulneración de seguridad?

El responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, con la finalidad de evitar que vuelva a ocurrir una vulneración.

¿A quién debo informar en caso de una vulneración?

Los responsables dentro del orden federal deberán notificar al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y a los titulares.
Al órgano garante deberá informar lo siguiente:

- Hora y fecha de la vulneración;
- Hora y Fecha del inicio de la investigación;
- Naturaleza de la vulneración ocurrida;
- La descripción de las circunstancias en torno a la vulneración;
- Las categorías y número aproximado de titulares afectados;
- Los sistemas de tratamiento y datos personales comprometidos;
- Las acciones correctivas realizadas;
- La descripción de las posibles consecuencias de la vulneración;
- Las recomendaciones dirigidas al titular;
- El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;

- El nombre completo de las personas designadas que puedan proporcionar mayor información al Instituto;
- Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

La notificación a los titulares por su parte deberá contener lo siguiente:

- La naturaleza de la vulneración;
- Los datos personales comprometidos;
- Las recomendaciones para que los titulares puedan proteger sus intereses;
- Las acciones correctivas realizadas;
- Los medios para que el titular pueda obtener mayor información;
- La descripción de las circunstancias generales en torno a la vulneración ocurrida.

Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

¿Cómo verificar el cumplimiento respecto al Sistema de Gestión?

Para conocer una lista de comprobación del contenido de los elementos que debe contener el Sistema de Gestión, dicho listado contempla: (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) los mecanismos de monitoreo y revisión de las medidas de seguridad, y (iv) el programa general de capacitación, se ponen a su disposición los anexos 6 del Documento orientador para la elaboración del Programa de Protección de Datos Personales, para lo cual podrá descargar el siguiente hipervínculo:http://inicio.ifai.org.mx/DocumentosdeInteres/AnexosDocumentoOrientador.zip y consultar específicamente los documentos:

- ANEXO6-MedidasdeSeguridad.docx (Paginas 20 a 22)
- ANEXO6-1-Vulneraciones.DOCX (Página 11)

En cuanto al análisis de riesgo, análisis de brecha, plan de trabajo, monitoreo y revisión de las medidas de seguridad, no se desarrollaron listas de comprobación, en razón de que se consideran elementos técnicos específicos.

VI. LOS DERECHOS ARCO

El acrónico ARCO está conformado por las iniciales de los derechos de Acceso, Rectificación, Cancelación y Oposición de los datos personales, derechos reconocidos por la legislación mexicana y que los titulares pueden ejercer, consisten en:

Derecho de Acceso Es el derecho que tiene el titular de solicitar el acceso a sus datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el tratamiento que se da a su información personal.

Por ejemplo: solicitar a una autoridad tributaria, acceso a sus datos de contacto que tenga registrados, para comprobar que los mismos sean correctos y estén actualizados.

Derecho de Rectificación Es el derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. En otras palabras, puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos sean incorrectos, desactualizados o inexactos. A manera de ejemplo: cuando un titular solicita un servicio a una Institución, el servidor público que atendió y registró, por error, un domicilio que no corresponde con el del titular, lo cual ha impedido notificar la solicitud de ratificación de su queja a la dirección correcta. Ante esa inexactitud, los titulares tienen el derecho de acudir a la Institución y solicitar la rectificación respectiva, acreditando el domicilio correcto.

Derecho de Cancelación Es el derecho que tienen los titulares de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los trata. Aunque hay que tomar en cuenta que no en todos los casos se podrán eliminar sus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.

Un ejemplo del ejercicio de este derecho es el siguiente: El responsable otorgaba una beca por un año, está ya concluyó, la institución sigue enviando trimestralmente un correo electrónico con una encuesta relacionada con la beca otorgada. A través del ejercicio del derecho de cancelación, el titular puede solicitar a la institución que borre su información de los registros, con la finalidad de ya no recibir dichos correos, pues ya concluyó la finalidad para la cual obtuvieron y trataron sus datos.

Derecho de Oposición Es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para una determinada finalidad, no para la totalidad de estas. También en este caso, como en el anterior, no siempre se podrá impedir el uso de los datos, cuento estos sean necesarios por motivos legales o para el cumplimiento de obligaciones.

Un ejemplo muy claro del ejercicio de este derecho, lo observamos cuando alguien manifiesta su oposición al tratamiento de sus datos personales cuando asistente a un curso en una Institución Gubernamental que imparte capacitación, recaba un correo electrónico el cual utiliza para enviar invitaciones a eventos y también para enviar un boletín informativo, el titular puede oponerse a una finalidad específica, pero desear recibir aún invitaciones para eventos futuros. A partir del ejercicio del derecho de oposición, el titular puede solicitar al responsable que no envié el boletín.

¿Existen limitantes para el ejercicio de los derechos ARCO?

Como cualquier otro derecho, el de protección de datos personales tiene límites, por lo que bajo ciertas circunstancias los derechos ARCO no podrán ejercerse o su ejercicio se verá limitado por cuestiones de seguridad nacional; orden, seguridad y salud públicos, así como por derechos de terceros.

Las causas por las que el responsable puede negar el ejercicio de los derechos ARCO[11] son:

- El titular de los datos personales o su representante no hayan acreditado su identidad;
- El responsable no es competente para atender la solicitud;
- Existe un impedimento legal;
- Se pueda afectar los derechos de terceras personas;
- Cuando el ejercicio de los derechos ARCO pudiera obstaculizar procesos judiciales o administrativos;
- Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
- Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
- Cuando los datos sean parte de información de las entidades sujetas a regulación y supervisión financiera del sujeto obligado, o
- Cuando en función de sus atribuciones del sujeto obligado, el uso, resguardo y manejo sean necesarios para mantener la integridad, estabilidad y permanencia del Estado mexicano.

Ahora bien, aunque no proceda el ejercicio de derechos ARCO, el responsable está obligado a responder la solicitud e informar las causas de improcedencia.

[11] Artículo 55 de la Ley General

¿Cómo se ejercen los derechos ARCO?

El derecho a la protección de datos personales es un derecho personalísimo, solamente los titulares o sus representantes podrán solicitar el ejercicio de los derechos ARCO, por lo que es indispensable acreditar la identidad.

Para que un derecho sea ejercido no es necesario que se haya ejercido previamente otro, ni el ejercicio de uno impide que posteriormente se ejerza uno distinto. Por ejemplo, un titular puede solicitar a una dependencia en su carácter de responsable la rectificación de sus datos personales sin que previamente haya ejercido su derecho de acceso, otro supuesto es que una persona puede solicitar la cancelación de sus datos, sin que haya accedido a estos.

¿Cuáles son los requisitos que debe tener una solicitud para el ejercicio de derechos ARCO?

La solicitud debe presentar ante el responsable que posea los datos personales respecto de los cuales requieras el acceso, rectificación, cancelación u oposición.

Los requisitos que debe tener la solicitud[12] son:

- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;
- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud; IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Con relación a los requisitos específicos, según el derecho que se quiera ejercer, están los siguientes:

Acceso: Debe indicar la modalidad en la que el titular prefiere que se reproduzcan los datos personales solicitados.

Rectificación: El titular debe especificar las modificaciones que se solicitan a los datos personales, así como aportar los documentos que sustenten la solicitud.

[12] Artículo 52 de la Ley General.

Cancelación: Deben señalar las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable.

Oposición: El titular debe manifestar las causas o la situación que llevan a solicitar que concluya el tratamiento de sus datos personales, así como el daño que le causaría que dicho tratamiento continúe. En el caso de que la solicitud se refiera a un tratamiento en lo particular, se deben indicar las finalidades específicas respecto de las cuales se solicita el ejercicio del derecho.

¿Cuál es la función de la Unidad de Transparencia en el ejercicio de los Derechos ARCO?

La Unidad de Transparencia deberá auxiliar al titular en la elaboración de las solicitudes para el ejercicio de derechos ARCO, así como informar sobre la obligación del titular de acreditar su identidad. Deberá atender a cada titular atendiendo su situación particular, facilitando la información que estos requieran.

Otra función de la unidad es cuando ya han recibido la solicitud y esta haya sido admitida deberá turnar la misma al área correspondiente que conforme a sus atribuciones, facultades, competencias o funciones puedan o deban poseer los datos.

¿Cómo se debe acreditar la identidad del titular y en su caso del representante?

Como se señaló anteriormente, un requisito fundamental para el ejercicio de derechos ARCO es que previamente se demuestre que quien desea ejercer el derecho, es el titular de los datos personales.

Para ello, es necesario que previo a que se ejerza el derecho de acceso, rectificación, cancelación u oposición se acredite la identidad del titular de los datos personales y de su representante, en caso de que la solicitud se realice por medio de este último, a través de la presentación de una identificación oficial.
Hay tres medios para acreditar la identidad:

- Identificación oficial
- Instrumentos electrónicos o mecanismos de autenticación, como la Firma Electrónica.
- Mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

Por su parte el representante deberá acreditar su personalidad mediante:

- Copia de identificación oficial del titular de los datos;
- Identificación del representante, y

- Instrumento notarial o Carta Poder (firmada por dos testigos y sus respectivas identificaciones)

¿Cómo deberá acreditar la personalidad en supuestos de menores de edad, en estado de interdicción o fallecidas?

Por su parte en el caso de las solicitudes de ejercicio de derechos ARCO de una persona menor de edad,[13] en estado de interdicción o incapacidad legal, o fallecida. Cuando se pretenda ejercer los derechos ARCO con relación a datos personales de una persona menor de edad o en estado de interdicción o incapacidad legal se deberá de observar lo dispuesto en las leyes civiles y la representación será conforme a las reglas que establezca dicha normatividad.

En cuanto a los datos personales de una persona fallecida, sólo la persona que acredite tener interés jurídico, conforme a las leyes aplicables, podrá ejercer los derechos ARCO, siempre que el titular de los datos personales hubiere expresado fehacientemente su voluntad o exista un mandato judicial al respecto, y se trate de una solicitud presentada ante un responsable del sector público.

En general, la representación de estas personas podrá acreditarse mediante los siguientes documentos:

Menores de edad:

En el caso de que los padres tengan la patria potestad del menor y sean los que deseen ejercer los derechos ARCO, además de acreditar la identidad del menor deberán presentar los siguientes documentos:

- Acta de nacimiento del menor de edad;
- Documento de identificación oficial del padre o de la madre que pretenda ejercer el derecho, y
- Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o madre, según sea el caso, ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

En los casos en que la patria potestad la ejerce una persona distinta a los padres, y es ella quien desea ejercer los derechos ARCO, además de acreditar la identidad del menor deberá presentar los siguientes documentos:

- Acta de nacimiento del menor de edad;
- Documento legal que acredite el ejercicio de la patria potestad;

[13] Acreditación de la personalidad en los artículos 78, 79 y 80 de la Ley General.

- Documento de identificación oficial de quien ejerce la patria potestad y presenta la solicitud, y
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

Cuando quien desee ejercer los derechos ARCO sea el tutor del menor de edad, además de acreditar la identidad del menor, deberá presentar los siguientes documentos:

- Acta de nacimiento del menor de edad;
- Documento legal que acredite la tutela;
- Documento de identificación oficial del tutor, y
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

Personas en estado de interdicción o incapacidad legal:

- Instrumento legal de designación del tutor;
- Documento de identificación oficial del tutor, y
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

Personas fallecidas:

- Acta de defunción;
- Documento(s) que acrediten el interés jurídico de quien presenta la solicitud, y
- Documento de identificación oficial de quien presenta la solicitud.

¿Cuál es el procedimiento y plazos a seguir en una solicitud de ejercicio de derechos ARCO?

El procedimiento inicia cuando el titular o su representante presentan la solicitud de ejercicio de derechos ARCO respecto de los datos personales de los cuales se requiere el acceso, rectificación, cancelación u oposición.

A continuación, se describe el procedimiento y plazos para la presentación y atención de las solicitudes de derechos ARCO:

Actividad Plazo para el titular:

Paso 1. Recepción de la solitud formulada por el titular o su representante.
* En cualquier momento.
La solicitud debe acusarse de recibida constando fecha de la misma.

Paso 2. Informará al titular si procede o no el ejercicio del derecho solicitado.
* 20 días hábiles.

Paso 3. En caso de que haya procedido el ejercicio del derecho, el responsable llevará a cabo las acciones necesarias para hacerlo efectivo.
* 15 días hábiles.
El plazo antes señalado se puede ampliar por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

Ahora bien, si la solicitud no cuenta con la información suficiente en su solicitud para el ejercicio de los derechos ARCO, entre el paso 1 y 2, el responsable podrá solicitar al titular que proporcione la información faltante por medio de un escrito denominado "prevención", el cual se deberá emitir en un plazo de máximo 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud. El titular contará con 10 días hábiles, después de recibir la prevención, para proporcionar la información requerida, pues de lo contrario se tendrá como no presentada su solicitud.

Recuerda que, aunque no proceda el ejercicio de los derechos ARCO, el responsable deberá responder la solicitud, explicando las causas de la improcedencia respectiva, en el plazo de 20 días hábiles señalado en el paso 2.

Por otra parte, toma en cuenta que cuando la normatividad aplicable a determinados tratamientos de datos personales establezca un trámite o procedimiento diferente para solicitar el ejercicio de derechos ARCO, procederá lo siguiente:

- El responsable deberá informar al titular sobre la existencia de dicho trámite o procedimiento en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, a fin de que el titular decida si presentará su solicitud de ejercicio de derechos ARCO de acuerdo con el trámite específico o con base en el procedimiento establecido en la ley.

¿Cuáles son los medios de presentación de la solicitud?

La solicitud se podrá presentar por escrito libre, formatos, medios electrónicos o cualquier otro que establezca el INAI o los Organismos garantes, en el ámbito de su competencia.

¿Tiene costo el ejercicio de derechos ARCO?

El ejercicio de los derechos ARCO es gratuito, y sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío de información, para ello hay determinadas reglas entre las que se encuentran las siguientes:

- Cuando el titular proporcione un medio magnético, electrónico o el mecanismo necesario para la reproducción de los datos personales, por ejemplo, un USB o un Disco Compacto, éstos deberán ser entregados sin costo.[14]
- La información deberá ser entregada sin costo cuando implique la entrega de no más de 20 hojas simples. [15]

¿Cuáles son las obligaciones vinculadas a los derechos ARCO?

Las obligaciones generales:

- Establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO.
- Los medios y procedimientos habilitados para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable.
- Establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.

¿Cómo verificar el cumplimiento respecto al ejercicio de derechos ARCO?

Para conocer más acerca del cumplimiento de sus obligaciones relacionadas con el ejercicio de derechos ARCO, así como acceder a un listado de comprobación relacionado con este tema se recomienda revisar el *"ANEXO7-DerechosARCO.DOCX del Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/AnexosDocumentoOrientador.zip

[14] Párrafo 3 del artículo 50 de la Ley General
[15] Párrafo 4, artículo 50 de la Ley General

VII. LA RELACIÓN ENTRE EL RESPONSABLE Y EL ENCARGADO Y LAS OBLIGACIONES QUE CUMPLIR

El encargado es un prestador de servicios que trata datos personales a nombre y por cuenta del responsable. Esta figura tiene las siguientes características:

- Puede ser una persona física o jurídica;
- Del ámbito público o privado;
- Ajeno a la organización del responsable, es decir, los trabajadores que forman parte de la estructura del responsable no son encargados;
- Puede tratar los datos solo o de manera conjunta con otras personas;

Por ejemplo: Si un organismo desconcentrado contrata a una empresa especializada en la elaboración de nóminas, y por virtud de la prestación del servicio, el sujeto obligado (responsable) le comunica los datos de los servidores públicos a dicha empresa para que elabore las nóminas y los recibos correspondientes, en este supuesto estaríamos hablando de que la empresa que elabora dichos documentos es la encargada del tratamiento.

Ahora bien, el responsable está obligado a establecer la relación con el encargado a través de un instrumento jurídico que permita acreditar la existencia de la relación jurídica, su alcance y contenido, como por ejemplo un contrato, cláusulas contractuales, acuerdos, convenios u otros instrumentos jurídicos. En todo caso, los acuerdos que se alcancen entre el responsable y el encargado deberán ser acordes con lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales y no deberá contravenir lo estipulado en la Ley General.

¿Qué obligaciones debe establecer el responsable en su relación con el encargado?

De acuerdo con el artículo 59 de la Ley General, el responsable deberá contemplar, al menos, las siguientes obligaciones del encargado en el instrumento jurídico en el que establezca la relación jurídica con éste:

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;

V. Guardar confidencialidad respecto de los datos personales tratados;

VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y

VII. 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

¿El encargado puede subcontratar servicios que impliquen tratamiento de datos personales?

En la práctica se dan habitualmente casos en los que hay una subcontratación de servicios, cuando el encargado del tratamiento tiene que recurrir a su vez a otras personas físicas o morales que le prestan algún servicio que implica el acceso a los datos personales del responsable.

De acuerdo con el numeral 61 de la Ley General, el encargado puede llevar a cabo subcontrataciones, siempre que cuente con la autorización del responsable, es decir, que se establezca en el instrumento jurídico mediante el cual se haya formalizado la relación entre responsable y encargado, se contemplen la subcontratación de servicios.

Una vez obtenida la autorización del responsable, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. Es importante que el encargado prevea en este instrumento que la persona subcontratada asuma las mismas obligaciones que se establezcan para el encargado.

Por ejemplo, si un responsable ha contratado a un encargado un servicio para la elaboración de nómina que implica el tratamiento de datos personales y este último hace uso de los servicios de otra persona jurídica para almacenar los datos personales en la nube, este último tratamiento de datos implica una subcontratación, que tendrá que estar autorizada por el responsable.

¿Qué pasa si el encargado incumple con la instrucción del responsable?

El **encargado será considerado responsable** de los datos personales en los casos en que incumpla con las instrucciones del responsable, contenidas en el instrumento jurídico que celebran previamente, siendo aplicables la normatividad de datos personales según corresponda, es decir, la Ley General o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

¿Qué pasa con el tratamiento de los datos personales en el servicio de cómputo en la nube?

De conformidad con la definición de la Ley General, se entiende por cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Cuando el responsable contrate o se adhiera a los servicios de cómputo en la nube, mediante cláusulas contractuales e instrumentos jurídicos.

Ahora bien, de conformidad con la normatividad aplicable para que el responsable se pueda adherir o celebrar un contrato para la prestación del servicio de cómputo en la nube, debe garantizar que el proveedor cumpla con las siguientes condiciones:

I. Cumpla, al menos, con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

II. Cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, y
e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

i. Obligaciones ligadas a la relación entre el responsable y el encargado:

De acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones respecto de la relación que establezca con los encargados que traten datos a nombre del responsable, deberán contar con lo siguiente:

1. La relación con los encargados debe formalizarse mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido.

2. Incluir en el contrato o instrumento jurídico, al menos las siguientes cláusulas con encargado:

   - El tratamiento de datos personales deber realizarse conforme a las instrucciones del responsable;
   - El encargado no debe tratar los datos personales para finalidades distintas a las instruidas por el Responsable;
   - El encargado debe Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
   - El encargado debe informar al responsable cuando suceda una vulneración a los datos personales.;
   - La obligación de guardar confidencialidad de los datos personales tratados;
   - Suprimir o devolver los datos personales una vez cumplida la relación jurídica salvo que exista una previsión legal que exija la conservación de los datos personales;
   - No debe el encargado transferir los datos personales, a menos que sea instrucción del responsable, o dicha comunicación derive de una subcontratación, o cuando derive de un mandato expreso de la autoridad competente;
   - Permitir al INAI o al Responsable, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales;
   - Colaborar con el INAI en las investigaciones previas y verificaciones de acuerdo a lo dispuesto en la Ley General y los Lineamientos Generales, el encargado tiene la obligación de proporcionar la información y documentación necesaria, y
   - El encargado para acreditar el cumplimiento de obligaciones puede generar, actualizar y conservar la documentación necesaria.

El responsable debe autorizar las subcontrataciones que realicen los encargados y que involucren el tratamiento de datos personales.

3. 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.

ii. ¿Cómo cumplo con las obligaciones derivadas de la relación con el encargado?

Para la revisión sobre el cumplimiento **de las obligaciones derivadas de la relación con el encargado** y acceder a un listado de comprobación relacionado con esta obligación, se recomienda revisar las **páginas 45 a 50** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

VIII. LAS TRANSFERENCIAS Y LAS OBLIGACIONES QUE CUMPLIR

La transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta del **titular, del responsable o del encargado**. Es decir, la comunicación de datos entre el responsable y el encargado, en el marco de la relación jurídica de la que se habló en el apartado anterior, **NO** se considera transferencia. A ese tipo de comunicaciones se les llama **remisiones**. Es importante señalar que los responsables no están obligados a solicitar el consentimiento de los titulares para la realización de remisiones, ni informarlas en el aviso de privacidad, contrario a lo que ocurre con las transferencias, como se verá más adelante.

Un ejemplo de transferencia sería cuando el responsable comunica los datos del servidor público al ISSSTE, a fin de que se otorguen las prestaciones que le corresponden por ley.

¿Cuáles son las condiciones generales para las transferencias?

Para que un responsable pueda transferir los datos personales, dentro o fuera de México, es necesario que:

1. Se informe al titular en el aviso de privacidad al destinatario de las transferencias ya sea en el ámbito público como privado, además deberá señalar las finalidades de estas transferencias. En caso de ser una transferencia que requiera consentimiento, deberá habilitar los mecanismos correspondientes.

2. El titular haya otorgado su consentimiento para que la transferencia se realice, salvo los casos de excepción previstos en el artículo 22, 66 y 70 de la Ley General (este tipo de transferencias es opcional incluirlas en el aviso de privacidad integral), y
No se requerirá el consentimiento de los titulares para realizar transferencias, algunos de los supuestos son:[16]

- Cuando una ley así lo disponga;
- Cuando las transferencias que se realicen entre responsables, para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- Para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica;
- Cuando exista una situación de emergencia;

[16] Se sugiere revisar los supuestos específicos contenidos en los artículos 22, 66 y 70 de la Ley General. El listado es de carácter ilustrativo, los supuestos específicos se encuentran en los numerales antes referidos.

- Asistencia sanitaria;
- Los datos se encuentren en fuentes de acceso público;
- Los datos personales sean sometidos a un procedimiento de disociación;
- El titular de los datos sea una persona reportada como desaparecida;
- Transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal;
- Transferencia sea internacional, en cumplimiento en una ley o tratado internacional suscrito y ratificado por el estado mexicano;
- A petición de una autoridad u organismo extranjero, competente en su carácter de receptor, cuyas facultades sean homologas;
- Transferencia necesaria por un contrato celebrado o por celebrar en interés del titular;
- La transferencia sea necesaria por razones de seguridad.

Por otra parte, el receptor en su carácter de responsable deberá cumplir con lo establecido en la normatividad aplicable en materia de datos personales, ya sea que pertenezca al sector público o privado.

¿Qué se requiere para llevar a cabo transferencias nacionales?

CONDICION ESPECIFICA	RECEPTOR DE LOS DATOS	FORMALIZACION
Cumplir con las condiciones generales para transferencias: ser informada en el aviso de privacidad; solicitar el consentimiento del titular cuando se requiera y limitarse a las transferencias consentidas e informadas.	El receptor de los datos personales adquirirá el carácter de responsable en términos de la Ley General, con las obligaciones respectivas. Este responsable deberá tratar los datos conforme a lo convenido en el aviso de privacidad que le comunique el responsable transferente.	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.

¿Qué se requiere para llevar a cabo transferencias internacionales?

CONDICION ESPECIFICA	RECEPTOR DE LOS DATOS	FORMALIZACION
Las transferencias internacionales serán posibles cuando el receptor de los datos asuma las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales. Asimismo, para que éstas ocurran será necesario cumplir con las condiciones generales para transferencias: ser informada en el aviso de	El receptor de los datos personales NO podrá considerarse un responsable en términos de la Ley General, pues al no estar establecido en territorio nacional, no le aplica la norma mexicana. No obstante, mediante el instrumento jurídico en el que se establezca la relación con el responsable que	El responsable transferente puede valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones para el tercero receptor, a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el

privacidad; solicitar el consentimiento del titular cuando se requiera y limitarse a las finalidades consentidas e informadas.	transfiere los datos personales, deberá asumir las mismas obligaciones que éste tiene con relación al tratamiento de los datos personales. Si el receptor de los datos no acepta estas condiciones, el responsable, a quien sí le aplica la ley mexicana, NO podrá transferirle los datos personales, pues de otra forma, él será quien incumpla con sus obligaciones legales.	tratamiento de sus datos personales.

En el caso de transferencias internacionales los responsables podrán solicitar la opinión del INAI, la solicitud debe contener los requisitos establecidos en el artículo 117 de los Lineamientos Generales.

¿A quién corresponde acreditar que se cumplió con las obligaciones en materia de transferencia?

La carga de la prueba para acreditar el cumplimiento de obligaciones en materia de transferencias de cualquier tipo corresponde exclusivamente al responsable.

i. Obligaciones ligadas a las transferencias:

El responsable tiene las siguientes obligaciones en torno a las transferencias de datos personales:

1. Todas las transferencias sean nacionales e internacionales deben formalizarse mediante la suscripción de un instrumento jurídico, para demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades contraídas las partes, salvo en las siguientes excepciones:

   - Cuando la transferencia sea nacional y se realice en virtud del cumplimiento de una disposición legal o en el ejercicio de las atribuciones expresamente conferidas.

   - Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o derivado de una petición de la autoridad extranjera u organismo internacional en su carácter de receptor, cuando las

facultades entre el sujeto obligado y el responsable receptor sean homólogas, o también, cuando las finalidades de la transferencia sean análogas respecto de aquéllas que dieron origen al tratamiento.

2. 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 Ley General y demás disposiciones aplicables en la materia.

3. Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen.

4. Solicitar el consentimiento para las transferencias nacionales e internacionales, salvo en los siguientes casos:

   - 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 se encuentre prevista en una ley o tratado suscrito y ratificado por México;
   - Cuando la transferencia sea entre responsables y derivado de sus atribuciones análogas o compatibles con la finalidad que dio origen al tratamiento;
   - No será necesario el consentimiento cuando se trate una transferencia legalmente exigida para la investigación y persecución de los delitos, o bien, la procuración o administración de justicia;
   - Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho;
   - Cuando la transferencia tenga como finalidad 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 en interés del titular, por el sujeto obligado y un tercero;
   - Cuando se trate de los casos en los que el Responsable 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 22 de la Ley General, y
   - Sea necesaria por razones de seguridad nacional.

5. El Responsable deberá establecer el medio para obtener el consentimiento expreso del titular de forma previa a la transferencia de los datos personales.

6. En caso de que la transferencia sea nacional, el receptor deber observar la confidencialidad y la obligación de utilizar los datos personales únicamente para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad

ii. ¿Cómo cumplo con las obligaciones derivadas de las transferencias?

Para la revisión sobre el cumplimiento **de las obligaciones derivadas de las transferencias** y acceder a un listado de comprobación relacionado con esta obligación, se recomienda revisar las **páginas 56 a 62** del *"Programa de Protección de Datos Documento Orientador"*, disponible en:

http://inicio.ifai.org.mx/DocumentosdeInteres/DocumentoOrientadorPPDP.docx

IX. ¿QUÉ PASA SI NO CUMPLO CON MIS OBLIGACIONES?

En caso de que los Sujetos Obligados en el ámbito federal en su calidad de responsables en el tratamiento de datos personales, incumplan con sus obligaciones, esto implica vulnerar el derecho humano a la protección de datos personales, que puede dar lugar a la imposición de medidas de apremio y sanciones.

EL INAI puede imponer como medidas de apremio la amonestación pública o una multa equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces del valor de la unidad de medida y actualización, estas multas no podrán ser cubiertas con recursos públicos.

Además, el incumplimiento será difundido en los portales de obligaciones de transparencia del INAI y serán considerados en la evaluación que éste realice. Cabe hacer mención que las medidas de apremio de carácter económico, es decir las multas no serán cubiertas con recursos públicos.

Existe el procedimiento de verificación a través del cual el INAI ejerce sus facultades para la vigilancia y verificación del cumplimiento de las disposiciones de la Ley General. Este procedimiento puede iniciar de oficio cuando el INAI presuma de manera fundada y motivada la existencia de incumplimiento a la Ley General, también puede iniciar por denuncia de los titulares que consideren que los responsables hayan realizado actos que puedan ser contrarios a lo dispuesto en la normatividad en materia de protección de datos personales.

El procedimiento de verificación concluye con una resolución del INAI, en la que se establecerán las medidas que correspondan.

En cuanto a las sanciones, serán causa el actuar o la omisión de los responsables de conformidad con el artículo 163 de la Ley General, lo siguiente:

- Actuar con negligencia, dolo o mala fe, dolo en el procedimiento para el ejercicio de los derechos ARCO;
- Por incumplimiento en los plazos para atención a las solicitudes para el ejercicio de los derechos ARCO;
- Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente los datos personales que se tengan en custodia;
- En forma intencional, tratar los datos personales violando los principios y deberes;
- No contar con el aviso de privacidad o no cuente con todos los elementos informativos;
- Clasificar como confidencial, con dolo o negligencia;
- Incumplir el deber de confidencialidad;

- No establecer las medidas de seguridad;
- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;
- No observar lo dispuesto en la Ley General en el caso de las transferencias;
- Obstruir los actos de verificación de la autoridad;
- Crear bases de datos personales en contravención a los dispuesto, para considerarse fuente de acceso público;
- No acatar las resoluciones emitidas por el INAI;
- Omitir la entrega del informe anual o entregarlo en forma extemporánea.

Cabe mencionar que la Ley General establece en el capítulo de Sanciones en los artículos 163 a 168, las causas por las cuales se puede considerar el incumplimiento a las obligaciones del responsable. En el supuesto de partidos políticos corresponderá a la autoridad electoral aplicar la medida de apremio que corresponda.

¿En caso de incumplimiento de obligaciones en materia de protección de datos personales, existe responsabilidad penal?

En caso de que el incumplimiento de las determinaciones de los Organismos garantes implique la presunta comisión de un delito o bien en alguno de los supuestos señalados previamente del artículo 163 de la Ley General, el organismo garante respectivo deberá denunciar los hechos ante la autoridad competente.

En la normatividad de la materia no se establecen capítulos o artículos específicos de la tipificación de un delito, corresponderá al tipo de conducta y la normativa específica por la materia o sector que se trate, para que pueda dar la configuración de un delito.

Por último, en caso de que se determine una violación a los supuestos mencionados el artículo 163 de la Ley General, con independencia de las sanciones administrativas, podrán derivar procedimientos de orden civil, penal o cualquier otro tipo.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales