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

Coordinación de Protección de Datos Personales

Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Junio de 2016

Contenido

GLOSARIO

Criterios Generales	Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos.
Derechos ARCO	Derechos de acceso, rectificación, cancelación y oposición.
DOF	Diario Oficial de la Federación.
INAI o Instituto	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Ley o LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Reglamento de la LFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

I. INTRODUCCIÓN

Con la publicación de la LFPDPPP[1] y su Reglamento,[2] las personas físicas o morales privadas, que traten datos personales en sus actividades, 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 el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que otorga el poder a toda persona física para que sus datos personales sean tratados de manera lícita y leal, a fin de garantizar su privacidad y derecho a la autodeterminación informativa, es decir, a decidir quién puede tratar sus datos personales y para qué fines.

Ya que se trata de un derecho humano recientemente regulado en nuestro país, y tomando en consideración que entre las atribuciones del INAI está proporcionar apoyo técnico para el cumplimiento de la Ley; se emite la presente guía, que busca:

- Facilitar el cumplimiento de la normatividad sobre 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 ayuda o apoyo para el cumplimiento de los principios y los deberes que establece la norma;
- Reducir el costo de la implementación de la normatividad básica sobre protección de datos personales, y
- 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 su posesión.

Es así que a continuación se desarrolla la guía para cumplir con las obligaciones de quienes tratan datos personales en el sector privado, en específico lo relativo a los ocho principios, los dos deberes, las transferencias y relación responsable-encargado.

[1] Publicada en el DOF de 5 de julio de 2010.
[2] Publicado en el DOF de 21 de diciembre de 2011.

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 por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que impone obligaciones a las personas físicas o morales que utilizan datos personales, y que otorga derechos a los titulares de los datos, a fin de garantizar el buen uso de la información personal y la privacidad y derecho a la autodeterminación informativa de las personas.

La autodeterminación informativa no es otra cosa más que 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 conlleva un riesgo que, en caso de mal uso, gestión o cuidado, puede 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 el debido tratamiento de la información.

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

2. ¿Qué es un dato personal?

Es cualquier información concerniente a una persona física identificada o identificable, como puede ser 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 o haga identificable al titular de los datos.

Los datos personales pueden estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otra modalidad.

Se considera que una persona es identificable cuando su identidad puede determinarse mediante los datos personales de que se traten.

La información relativa a una persona moral no se considera como dato personal, quedando ésta excluida de la protección que otorga la normatividad sobre protección de datos personales a las personas físicas.

Es importante considerar que si los datos personales son objeto del procedimiento de disocian, de forma tal que no es posible asociarse a su titular, ni permitir su identificación, dejarán de ser

considerados como tales y, por lo tanto, no será aplicable la normatividad sobre protección de datos personales.

3. ¿Qué es un dato personal sensible?

Son datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen o conlleve un riesgo grave para éste, como por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

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

Tratar datos personales es un concepto amplio, ya que incluye:

El uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Por ejemplo, un responsable del tratamiento puede obtener datos personales de una persona física, a través de un formulario en papel, almacenarlos en el disco duro de una máquina o en la nube, utilizarlos para sus actividades cotidianas, 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, es el dueño de los datos personales, 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?

Es la persona física o moral de carácter privado **que decide** sobre el tratamiento de los datos personales, es decir, la que 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.

El responsable del tratamiento puede ser, por ejemplo, una empresa o persona moral, un emprendedor, un doctor, un abogado, un contador, una organización de la sociedad civil, una escuela o colegio, el patronato de un museo, una universidad privada o una fundación, o cualquier otra persona física o moral que decida sobre el tratamiento de los datos personales para el desarrollo de su actividad.

7. ¿Quién es el encargado del tratamiento?

Es la persona física o moral, 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, se considera encargado a la empresa que fue contratada por el responsable para administrar su nómina o prestarle el servicio de *call center*. También sería encargada del tratamiento una empresa que ofrece servicios de cómputo en la nube y que almacena bases de datos de un responsable, o bien, aquélla que contrató el responsable para la destrucción de sus documentos.

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 LFPDPPP, en caso de incumplimiento.

8. ¿A quién le aplica la Ley?

La LFPDPPP aplica a TODAS las personas físicas o morales de carácter privado, que en el desarrollo de sus actividades traten datos personales, con excepción de los únicos dos supuestos previstos en su artículo:

1) Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
2) Las personas físicas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Entonces, sólo en los dos supuestos antes señalados no aplicará la LFPDPPP. En todos los demás casos en los que un particular trate datos personales aplicará la norma, por ejemplo, a los notarios,

abogados, contadores, médicos, organizaciones de la sociedad civil, empresas, bancos, aseguradoras, escuelas, entre otros.

Por su parte, el artículo 5 del Reglamento de la LFPDPPP establece que la norma no será aplicable a la siguiente información:

- La relativa a personas morales;
- Aquélla que refiera a personas físicas en su calidad de comerciantes y profesionistas, y
- La de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono y número de fax; siempre que esta información sea tratada para fines de representación del empleador o contratista.

En ese sentido, tenemos que la LFPDPPP además de no aplicar a las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia, ni a las personas físicas que traten datos personales para uso exclusivamente personal; sus disposiciones no resultan aplicables a la información a la que refiere el artículo 5 de su Reglamento.

En suma, el artículo 2 de la LFPDPPP establece excepciones a su aplicación para personas físicas y morales, mientras que el artículo 5 del Reglamento de la LFPDPPP señala excepciones a su aplicación con relación a cierta información.

9. ¿Cuál es el ámbito objetivo de aplicación de la Ley?

La Ley, su Reglamento y demás normatividad que derive de éstos, 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 anterior implica que si no es posible acceder a los datos con base en estos criterios y, por tanto, para ello se requieren plazos o actividades desproporcionadas, en esos casos, no aplicará la norma que regula la protección de los datos personales.

Por otra parte, para que la normativa en materia de datos personales aplique no es indispensable que los datos personales se encuentren en un formato en lo específico, ya que éstos pueden estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otro tipo. Lo importante es que se trate de información concerniente a una persona física identificada o identificable.

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

La LFPDPPP es de observancia general en toda la República Mexicana, por lo que es la única ley que regula el tratamiento de datos personales en posesión de los particulares en el país. En ese sentido, no existen leyes locales para esta materia que apliquen al sector privado, con independencia de que las haya para regular el tratamiento de datos personales en posesión del sector público.

La LFPDPPP aplica en cualquiera de los siguientes casos:

- El tratamiento de datos personales se realice en un establecimiento del responsable ubicado en territorio mexicano.
- El tratamiento lo realice un encargado a nombre de un responsable establecido en territorio mexicano, sin importar dónde se encuentre ubicado dicho encargado, ya que quien responde por el debido tratamiento de los datos personales es el responsable.
- El responsable no esté establecido en territorio mexicano pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional.
- El responsable no esté establecido en territorio mexicano pero utilice para el tratamiento medios situados en el país, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento. En este caso, el responsable deberá proveer los medios necesarios para que los datos personales se traten conforme a la legislación mexicana, para lo cual, por ejemplo, podrá designar un representante en territorio nacional.

Asimismo, es importante señalar que cuando el responsable no se encuentre ubicado en territorio mexicano, pero el encargado lo esté, a este último le serán aplicables las disposiciones relativas a las medidas de seguridad previstas por la normativa en materia de protección de datos personales, así como el resto de las obligaciones que con relación al encargado establezca la LFPDPPP, su Reglamento y demás normativa aplicable.

11. ¿Qué es una transferencia de datos personales?

Se denomina transferencia de datos personales a la comunicación de datos que realiza el responsable del tratamiento a un tercero, **distinto del titular, del mismo responsable (por ejemplo las comunicaciones al interior de la organización del responsable, como las que se realizan entre el personal) 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

VII de esta guía. No obstante, en ambos casos, es necesario que se cumpla con todos los principios de la protección de datos, deberes y derechos que establece la norma mexicana.

Ejemplos de transferencias:

- Un patrón o una empresa (responsable del tratamiento) que comunica datos personales de sus trabajadores al Instituto Mexicano del Seguro Social (tercero), para el cálculo de la pensión.
- Una empresa del grupo corporativo A (responsable) comunica datos de sus clientes a otra empresa del mismo grupo (tercero), a fin de que esta última pueda ofrecer sus servicios.
- Un hospital (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 mexicana (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?

Al igual que en el caso de la transferencia, la remisión 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, como se verá más adelante, 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:

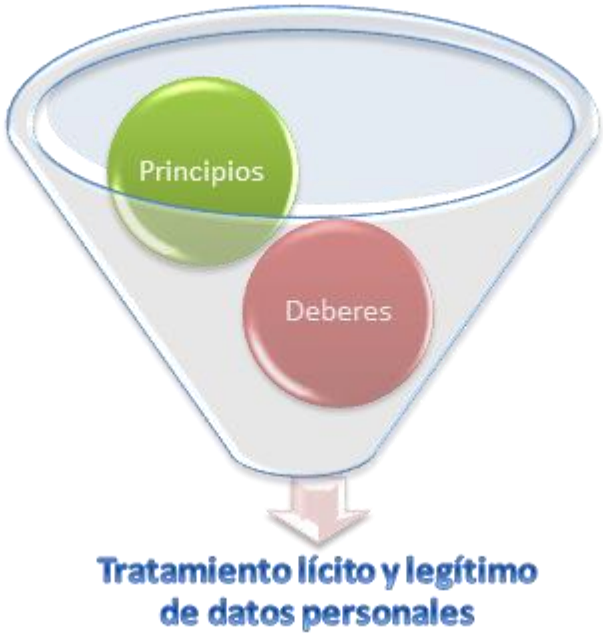
- Una empresa comunica datos personales a un contador que le presta los servicios de elaboración de su nómina.
- Un banco comunica datos de contacto de sus clientes a un *call center* ubicado fuera del país, para que le preste el servicio de atención de quejas.
- Una institución financiera comunica datos 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

El objeto de la LFPDPPP es 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 los deberes de seguridad y confidencialidad se convierten en obligaciones concretas para el responsable, que tiene que cumplir, así como hacer cumplir, en cada una de las fases del tratamiento.



Ahora bien, para cumplir con estas obligaciones, en primer lugar, resulta importante que el responsable conozca cómo se 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, se sigue con respecto al tratamiento de los datos personales (DP), desde que éstos se recaban hasta que los mismos se eliminan de sus bases de datos.

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

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

1. ¿Mi organización trata datos personales en el ejercicio de sus actividades cotidianas?
Nota: recuerde 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 su organización debe cumplir con las obligaciones que establece la LFPDPPP, según si es encargado o responsable.

2. ¿Qué figura tiene mi organización? ¿es responsable o encargado?
Nota: recuerde que el responsable es la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. Un encargado es la persona física o moral que sola o conjuntamente con otras trata datos personales a nombre y por cuenta del responsable.

3. ¿Qué tipo de datos personales trata mi organización?
Nota: se sugiere hacer un listado de TODOS los datos personales que se recaban y utilizan para las distintas actividades de la organización.

4. ¿Alguno de estos datos personales son patrimoniales, financieros o sensibles?
Nota: recuerde que los datos personales sensibles son aquéllos que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, como por ejemplo: origen racial o étnico de una persona, su estado de salud, su información genética, sus creencias religiosas, filosóficas o morales, su afiliación sindical, sus opiniones políticas o su preferencia sexual.

5. ¿De dónde se obtienen los datos personales?
Nota: 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 consultorio médico (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 obtienen 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, diario oficial, entre otros) o la persona física o moral que los comunica a la organización.

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 o el Registro Nacional de Profesionistas de la Secretaría de Educación Pública.

6. ¿Qué persona, área o departamento de la organización trata los datos personales?
Nota: recuerde que por tratamiento se entiende la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales. En ese sentido, se deberán

identificar las personas, áreas o departamentos de la organización 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.

7. ¿Para qué fines se tratan los datos personales?
Nota: 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 o servicios concretos que brinda la organización.

8. ¿Se comunican datos personales a encargados?
Nota: recuerde que un encargado es la persona física o moral que sola o conjuntamente con otras trata datos personales a nombre y por cuenta del responsable, por ejemplo un *call center* que ofrece publicidad a nombre del responsable o una empresa contratada por el responsable para administrar su nómina o prestarle el servicio de facturación electrónica.

9. ¿Se comunican datos personales a personas físicas o morales que no sean encargados? ¿a quién y para qué se comunican los datos?
Nota: recuerde que las comunicaciones de datos personales a personas distintas al responsable, titular o encargado se llaman transferencias. Es necesario identificar a quién se comunican los datos personales y para qué fines.

10. ¿Dónde se almacenan los datos personales?
Nota: Los datos personales que trata pueden estar almacenados en soporte electrónico o físico.

11. ¿Por cuánto tiempo se conservan los datos personales?
Nota: Si aún no tiene definido los plazos de conservación, más adelante le daremos algunas recomendaciones para hacerlo.

12. ¿Cómo se borran o eliminan los datos personales?
Nota: identifique los medios que utiliza para el borrado o eliminación de los datos personales.

Una vez realizado el diagnóstico del tratamiento de datos personales que se efectúa en la organización del responsable, es posible, ahora sí, identificar cómo cumplir con las obligaciones que establece la normativa que regula la protección de datos personales en nuestro país.

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:

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. Principios de licitud y lealtad

Los datos personales tienen que ser tratados por el responsable de manera lícita y leal, lo que supone que tiene que actuar con apego a las leyes en general y en lo particular a la normatividad sobre protección de datos personales. En ese sentido, el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido.

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 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.

1.1 Obligaciones ligadas a los principios de licitud y lealtad:

En resumen, de acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno a los principios de licitud y lealtad:

1. Tratar siempre los datos personales con apego al cumplimiento de la legislación mexicana y el derecho internacional;
2. No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales, y
3. Respetar en todo momento la expectativa razonable de privacidad del titular.

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

1.2 ¿Cómo cumplo con los principios de licitud y lealtad?

Obligación	Acciones recomendadas para el cumplimiento
Tratar siempre los datos personales con apego a la legislación mexicana y el derecho internacional	• Revisar que los datos se traten conforme a la LFPDPPP, su Reglamento y demás normativa aplicable. • Conocer la normativa que en lo particular regule la actividad en la que se tratan los datos personales, como por ejemplo las disposiciones en materia de salud o

	bancarias, e identificar si dicha normativa incluye disposiciones que se vinculen, de manera directa o indirecta, con la protección o el tratamiento de datos personales. • Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.
No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales	• Revisar los procedimientos y formatos utilizados por la organización o por los encargados contratados para recabar datos personales, para verificar que en éstos no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia. Por ejemplo, se pueden realizar acciones de capacitación y concientización del personal, y prohibir cláusulas contractuales o mecanismos de otro tipo que conduzcan a la obtención de datos personales por medios engañosos o fraudulentos. • Prever sanciones para el personal o encargados en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales.
Respetar en todo momento la expectativa razonable de privacidad de los titulares, privilegiando su protección en el tratamiento de sus datos personales	• Tratar los datos conforme lo acordado e informado al titular, en los términos de la normatividad aplicable y el aviso de privacidad.

1.3 Lista de comprobación para los principios de licitud y lealtad (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Conoce la LFPDPPP, su Reglamento y la normativa que deriva de la misma y ha identificado sus obligaciones?			
2	¿Conoce la normativa que en lo particular regula la actividad en la que se tratan los datos personales y ha identificado aquellas disposiciones que pudieran estar vinculadas con el tratamiento de datos personales?			

3	¿Ha verificado que en su organización los datos personales se traten conforme a la normativa señalada en las preguntas 1 y 2?			
4	¿Se asegura de que no se obtengan datos personales a través de medios engañosos o fraudulentos?			
5	¿Se asegura de que la información proporcionada al titular sobre el tratamiento de sus datos personales, a través del aviso de privacidad, es veraz y completa?			
6	¿Se asegura que los datos personales son tratados conforme a lo informado y acordado con el titular?			
7	¿Ha adoptado medidas que permitan verificar el cumplimiento de los principios de licitud y lealtad?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con los principios de licitud y lealtad.

2. 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 publicidad de los servicios deportivos que ofrece la organización.
> 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.

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 3 de este apartado -Principio de información-, se explicará lo relativo al aviso de privacidad).

¿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 datos patrimoniales, financieros y 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 datos financieros y patrimoniales.	El titular deberá expresamente señalar que consiente el tratamiento de sus datos personales. Por ejemplo: □ *Consiento que mis datos personales sean tratados para las finalidades antes descritas.* En el caso del consentimiento expreso, por fuerza, el titular deberá indicar en la casilla que consiente el tratamiento de sus datos personales, pues si no existe esa manifestación expresa, el responsable no podrá tratar los datos personales. En ese sentido, es necesario que el titular explícitamente diga que sí.
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.

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 financieros, patrimoniales o 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 patrimoniales y financieros tendrá que solicitar el consentimiento expreso, y de datos personales sensibles, el expreso y por escrito, cuando no se actualice alguno de los supuestos previstos en el artículo 10 de la LFPDPPP.

¿Cómo se obtiene el consentimiento tácito de los titulares si no existe contacto con ellos?
De acuerdo con lo señalado por el segundo párrafo del artículo 14 del Reglamento de la LFPDPPP, 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.

¿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 LFPDPPP en su artículo 10, los cuales son los siguientes:

- Cuando el tratamiento sea necesario porque así lo ordena una ley;
- Los datos personales se obtengan de una fuente de acceso público;
- Los datos personales se sometan a un procedimiento previo de disociación, de forma tal que no se pueda identificar su titular;
- El tratamiento tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable, por ejemplo, la relación entre un doctor y su paciente;

- Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- Los datos personales sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables, y que el tratamiento se realice por una persona sujeta al secreto profesional u obligación equivalente, o
- Se dicte resolución de autoridad competente.

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.

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 envío del 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 la organización 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 10 de la LFPDPPP, 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.

2.1 Obligaciones ligadas al principio de consentimiento:

En resumen, de acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno al principio de consentimiento:

1. Obtener el consentimiento del titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos previstos en el artículo 10 de la LFPDPPP;
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 para los datos personales financieros o patrimoniales, en los casos que no se actualice alguna de las causales del artículo 10 de la LFPDPPP;
5. 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 10 de la LFPDPPP;
6. 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;
7. Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento;
8. 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 10 de la LFPDPPP;
9. 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 10 de la LFPDPPP;
10. 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);
11. 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;
12. Esperar el plazo de cinco días hábiles que señala el artículo 14 del Reglamento de la LFPDPPP, 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;

13. Generar pruebas para acreditar que se cumplió con el principio de consentimiento, y
14. 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 10 de la LFPDPPP.

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

2.2 ¿Cómo cumplo con el principio de consentimiento?

Obligación	Acciones recomendadas para el cumplimiento
Obtener el consentimiento del titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos previstos en el artículo 10 de la Ley.	• Elaborar un listado con todas las finalidades para las cuales la organización trata los datos personales. • Verificar e identificar para cuáles de esas finalidades se requiere el consentimiento, a partir de los supuestos de excepción que establece el artículo 10 de la LFPDPPP. • Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.
Solicitar el consentimiento siempre ligado a finalidades específicas, informadas en el aviso de privacidad.	• Verificar que todas las finalidades sean concretas y se encuentren contenidas en los avisos de privacidad respectivos.
Determinar el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito. Solicitar el consentimiento expreso para los datos personales financieros o patrimoniales, y el expreso y por escrito para los datos personales sensibles, siempre y cuando no se actualice alguno de los supuestos del artículo 10 de la LFPDPPP. Solicitar el consentimiento expreso o expreso y por escrito cuando así lo requiera una ley o	• Una vez que se ha identificado para cuáles finalidades se requiere consentimiento, hay que definir en cuáles aplica el tácito y en cuáles se requiere el expreso o expreso y por escrito. • Para ello, es necesario que se identifique en cuáles se tratan datos personales financieros o patrimoniales (consentimiento expreso) y en cuáles sensibles (consentimiento expreso y por

Obligación	Acciones recomendadas para el cumplimiento
reglamento, se acuerde con el titular o lo determine conveniente el responsable.	escrito). En todos los demás casos será suficiente con el tácito. • Verificar en las leyes que regulen en lo específico el tipo de tratamientos que lleva a cabo la organización, si se requiere un tipo de consentimiento en lo particular. • Determinar si por alguna razón en lo particular es conveniente solicitar el consentimiento expreso o expreso o por escrito, a pesar de que no lo exija una ley o no se trate de datos personales patrimoniales, financieros o sensibles. • Identificar los casos en los que por alguna cuestión en lo particular se haya acordado con el titular, obtener el consentimiento expreso o expreso y por escrito.
Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento.	• Verificar que los procedimientos de la organización establezcan que previo a solicitar el consentimiento de los titulares, se requiere poner a su disposición el aviso de privacidad.
Solicitar el consentimiento previo a la obtención de los datos personales, si éstos se recaban directamente del titular.	• Verificar que los procedimientos de la organización establezcan que previo a la obtención de los datos personales, es necesario obtener el consentimiento de los titulares para los tratamientos descritos en el aviso de privacidad.
Solicitar el consentimiento antes de utilizar los datos personales para las finalidades para las cuales se obtuvieron, si éstos se recabaron de manera indirecta.	• Cuando se requiera el consentimiento tácito: llevar un control de aquellos casos en los que se envíe el aviso de privacidad por un medio que NO permita el contacto directo con los titulares (por ejemplo, correo postal), registrar la fecha de envío, y esperar cinco días hábiles, para poder tratar los datos personales en caso de que el titular no

Obligación	Acciones recomendadas para el cumplimiento
	haya manifestado su negativa en ese plazo. En los casos en que el aviso de privacidad se haya dado a conocer por un medio que permita el contacto directo (por ejemplo correo electrónico o teléfono), verificar que el titular no haya manifestado su negativa para el tratamiento de los datos personales. • Cuando se requiera el consentimiento expreso o expreso y por escrito: llevar un control del envío o puesta a disposición del aviso de privacidad a los titulares y de la solicitud de consentimiento, y esperar hasta recibir el consentimiento por parte del titular, para poder tratar los datos personales. Si el responsable nunca recibe el consentimiento expreso o expreso y por escrito, no podrá tratar los datos personales.
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).	• Si se requiere el consentimiento tácito, será necesario que los procedimientos de la organización establezcan que antes de solicitar el consentimiento se haga del conocimiento del titular el aviso de privacidad, y que se registren aquellos casos en los que los titulares no otorguen su consentimiento. • Si se requiere el consentimiento expreso, se deberán habilitar mecanismos para que el titular expresamente pueda decir que SÍ otorga su consentimiento, como por ejemplo casillas de marcación en formatos impresos o electrónicos, o grabaciones telefónicas en las que el

Obligación	Acciones recomendadas para el cumplimiento
	titular pueda elegir un medio que indique que otorga su consentimiento. • Si se requiere el consentimiento expreso y por escrito, se deberán habilitar medios para que el titular manifieste su consentimiento a través de su firma autógrafa, electrónica, huella dactilar u otro permitido por la ley.
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.	• Elaborar listados para identificar plenamente a los titulares que negaron su consentimiento para el tratamiento de los datos personales, así como a las finalidades para las cuales negaron su consentimiento, ya que es posible que para algunas finalidades hayan otorgado su consentimiento, pero para otras no. • El objeto de los listados será evitar que los datos personales sean tratados sin el consentimiento de su titular, por lo que deberán estar elaborados de forma tal que permitan llevar de manera eficiente el control.
Esperar el plazo de cinco días hábiles que señala el artículo 14 del Reglamento de la LFPDPPP.	• Incluir la información relativa a este plazo en el aviso de privacidad. • Llevar un control con relación a la fecha en que se envió el aviso de privacidad y el término del plazo de cinco días hábiles. • No tratar los datos personales para estas finalidades antes de que concluya el plazo respectivo. • Si una vez concluido el plazo de cinco días e iniciado el tratamiento por parte del responsable, éste recibiera una negativa para el tratamiento por parte de un titular, se deberá concluir el tratamiento respectivo.

Obligación	Acciones recomendadas para el cumplimiento
Generar pruebas para acreditar que se cumplió con el principio de consentimiento.	• Cuando se requiera el consentimiento expreso y expreso y por escrito: conservar el documento, físico o electrónico, que permita acreditar que se obtuvo el consentimiento del titular. • Cuando se requiera el consentimiento tácito: contar con los medios que permitan acreditar que el aviso de privacidad se puso a disposición del titular, 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.
Solicitar el consentimiento si hubo cambio en las finalidades informadas en el aviso de privacidad.	• Verificar si para las nuevas finalidades es necesario obtener el consentimiento. • Si el consentimiento se requiere, será necesario poner a disposición de los titulares el nuevo aviso de privacidad. Si no se requiere el consentimiento, será suficiente con informar sobre los cambios en el aviso de privacidad (ver principio de información). • Solicitar el consentimiento de acuerdo con la modalidad que se requiera: tácito, expreso o expreso y por escrito.

2.3 Lista de comprobación para el principio de consentimiento (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Se ha verificado para qué finalidades se requiere el consentimiento, de acuerdo con lo dispuesto por el artículo 10 de la LFPDPPP?			
2	¿El consentimiento se solicita con relación a finalidades concretas informadas en el aviso de privacidad?			
3	¿Se ha definido qué tipo de consentimiento se requiere: tácito, expreso o expreso y por escrito?			
4	¿Se da a conocer el aviso de privacidad previo a la solicitud del consentimiento?			

5	Cuando los datos se obtienen directamente del titular ¿Se solicita el consentimiento previo a la obtención de los datos personales?			
6	Cuando los datos se obtienen de manera indirecta, el aviso de privacidad se da a conocer por un medio directo (por ejemplo correo electrónico o teléfono) y se requiere el consentimiento tácito ¿se verifica que el titular no haya negado su consentimiento para el tratamiento de sus datos personales?			
7	Cuando los datos se obtienen de manera indirecta, el aviso de privacidad se da a conocer por un medio indirecto (por ejemplo correo postal) y se requiere el consentimiento tácito ¿se tiene establecido un procedimiento para esperar el plazo de 5 días hábiles para el tratamiento de los datos personales?			
8	Cuando los datos se obtienen de manera indirecta y se requiere el consentimiento expreso o expreso y por escrito ¿se da a conocer el aviso de privacidad correspondiente, se solicita el consentimiento al titular y se espera a su obtención para el tratamiento de los datos personales?			
9	¿Los medios implementados para la obtención del consentimiento son sencillos y gratuitos y acordes con el tipo de consentimiento que se requiere?			
10	¿Se cuenta con listados para llevar un control de los titulares que han negado su consentimiento y de las finalidades para las cuales no podrán ser tratados los datos personales?			
11	¿Se generan pruebas para demostrar el cumplimiento del principio de consentimiento?			
12	En caso de que haya habido cambios en las finalidades y se requiera el consentimiento ¿se solicita el consentimiento y se da a conocer el nuevo aviso de privacidad?			
13	¿Se lleva un control sobre el plazo de cinco días hábiles que se debe esperar para el tratamiento de los datos personales cuando esta espera es necesaria?			
14	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de consentimiento?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con el principio de consentimiento.

3. Principio de información

Por virtud de este principio, los responsables se encuentran obligados a informar a los titulares de los datos personales, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad. En ese sentido, todo responsable que trate datos personales, sin importar la actividad que realice o si se trata de una persona física o moral, 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 para el tratamiento relativo al personal del responsable y otro para sus clientes.

La puesta a disposición del aviso de privacidad implica **hacer del conocimiento** del titular dicho documento. En ese sentido, el responsable no está obligado a entregar una copia del aviso de privacidad al titular, al menos que éste lo solicite.

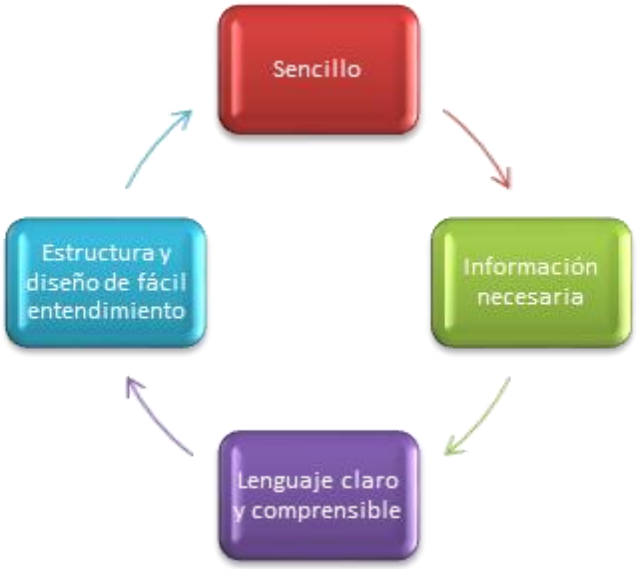
Con objeto de cumplir con esta obligación, el Instituto ha elaborado y puesto a disposición en su portal de Internet las siguientes herramientas:

1. El Generador de Avisos de Privacidad (GAP);
2. La guía El ABC del Aviso de Privacidad;
3. El formato de auto-evaluación de avisos de privacidad para responsables;
4. Modelo de aviso de privacidad corto para video vigilancia; y
5. Modelo de aviso de privacidad simplificado en video.

Estos cinco instrumentos se elaboraron con la finalidad de orientar a los responsables en la elaboración de sus avisos de privacidad, por lo que se les invita a acceder a los mismos a través del sitio www.inai.org.mx.

En particular, se sugiere hacer uso del GAP, que es una herramienta informática gratuita que permite a cualquier micro, pequeña, mediana o gran empresa elaborar y actualizar los avisos de privacidad que correspondan a los tratamientos de datos personales que lleven a cabo, con plena observancia de todos y cada uno de los elementos informativos a que se refiere la Ley, su Reglamento y los Lineamientos del Aviso de Privacidad. El GAP se encuentra disponible a través del siguiente vínculo electrónico: http://generador-avisos-privacidad.inai.org.mx/.

¿Qué características debe tener un aviso de privacidad?



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

- Abstenerse 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 responsable puede utilizar el medio que considere conveniente para difundir su aviso de privacidad, pero debe tener en cuenta que este medio debe estar acorde con la forma en que obtiene los datos personales y la modalidad de aviso de privacidad que utilice. En todo caso, el aviso de privacidad deberá estar ubicado en un lugar visible y que facilite su consulta.

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
Cualquier otra tecnología	

¿Cuáles son las modalidades del aviso de privacidad?

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

¿Qué elementos informativos debe contener cada una de las modalidades del aviso de privacidad?

ELEMENTO INFORMATIVO	INTEGRAL	SIMPLIFICADO	CORTO
I. La identidad y domicilio del responsable que trata los datos personales;	✓	✓	✓
II. Los datos personales que serán sometidos a tratamiento;	✓	—	—
III. El señalamiento expreso de los datos personales sensibles que se tratarán;	✓	—	—
IV. Las finalidades del tratamiento;	✓	✓	✓
V. Distinguir entre las finalidades que son necesarias y dieron origen a la relación jurídica, de las que no lo son;	✓	✓	—
VI. Los mecanismos para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable;	✓	✓	—
VII. Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas;	✓	—	—
VIII. La cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera;	✓	—	—
IX. Los medios y el procedimiento para ejercer los derechos ARCO;	✓	—	—
X. Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales;	✓	—	—
XI. Las opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de los datos personales;	✓	—	—
XII. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra	✓	—	—

tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso;			
XIII. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad;	✓	—	—
XIV. Los mecanismos para que el titular conozca el texto completo del aviso de privacidad **integral**.	—	✓	✓

¿Cuándo puedo hacer uso de cada una de las modalidades de aviso de privacidad?
El uso de las modalidades integral, simplificado o corto va a depender de la forma en que se obtengan los datos personales, tal y como a continuación se detalla:

Modalidad	¿Cuándo se pone a disposición?
Integral	Cuando los datos se obtengan personalmente del titular, por ejemplo, en una entrevista presencial.
Simplificado	Cuando los datos se obtienen de manera directa del titular, por ejemplo, el registro en una página de Internet o cuando se recaban datos vía telefónica.
Corto	Cuando el espacio para dar a conocer el aviso de privacidad sea limitado y los datos personales recabados sean mínimos, ejemplo, el cajero automático, un mensaje SMS o el boleto de una rifa.

¿En qué momento se debe poner a disposición del titular el aviso de privacidad?
Al igual que en la elección de la modalidad de aviso de privacidad, el momento en que éste se debe poner a disposición del titular depende de la forma en que se obtienen los datos personales, como se muestra a continuación:

MOMENTO DE LA PUESTA A DISPOSICIÓN	FORMA DE OBTENCIÓN DE LOS DATOS
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

MOMENTO DE LA PUESTA A DISPOSICIÓN	FORMA DE OBTENCIÓN DE LOS DATOS
	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	**Indirecta.** Ver inciso B. Ahora bien, a diferencia del caso expuesto en el inciso anterior, en este supuesto, el tratamiento de los datos personales no involucra el contacto con los titulares, por lo que la puesta a

MOMENTO DE LA PUESTA A DISPOSICIÓN	FORMA DE OBTENCIÓN DE LOS DATOS
	disposición del aviso de privacidad no puede ser al primer contacto. Por ejemplo, los datos se obtuvieron de una fuente de acceso público y se utilizarán para un estudio, en el que no se requiere entrar en contacto con los titulares. **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	**Personal o directa.** Ver inciso A. 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.**

¿Qué pasa cuando se hace uso de *cookies, web beacons* u otras tecnologías similares?
Las *cookies*, *web beacons* y otras tecnologías similares son herramientas utilizadas en páginas de Internet que permiten la obtención de datos personales de manera automática al tiempo que el titular visita dichas páginas.

Se considera que estas tecnologías tratan datos personales cuando es posible identificar o hacer identificable al titular de la información que se recaba.
Cuando estas tecnologías son utilizadas por el responsable, éste debe informar al titular, al momento en que ingrese a su portal de Internet, lo siguiente: que se están usando esas tecnologías de rastreo, que con ellas se obtienen datos personales y la forma en que se podrán deshabilitar, a menos que sean necesarias por motivos técnicos.

Además de informar lo anterior en el momento en que el titular tiene contacto con el portal de Internet del responsable, en los casos en que se obtienen datos personales en el portal de Internet, adicionales a los que se recaban a través de las tecnologías de rastreo (por ejemplo mediante el llenado de un formulario para la prestación de un servicio), y en ese sentido el aviso de privacidad se dé a conocer por Internet, el responsable deberá incluir en su aviso de privacidad la información descrita en el párrafo anterior y aquélla que deba incluirse en el aviso de privacidad, entre ella, los datos personales que se recaban y las finalidades del tratamiento.

¿El responsable está obligado a demostrar el cumplimiento de la obligación 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.

¿Existen excepciones al principio de información?
El responsable **no** está obligado a dar a conocer el aviso de privacidad en los siguientes casos:

- Cuando obtenga los datos personales de forma indirecta y éstos se encuentren destinados a fines históricos, estadísticos o científicos.
- Cuando recabe información de personas morales, ya que en México el derecho a la protección de datos personales sólo aplica a personas físicas.
- Cuando obtenga datos personales de personas físicas en su calidad de comerciantes y profesionistas, por ejemplo, de un proveedor.
- Cuando obtenga datos con fines de representación de personas físicas que prestan sus servicios a otras personas físicas o morales, relativos al nombre completo, puesto desempeñado, domicilio físico, correo electrónico, teléfono y número de fax, por ejemplo, una tarjeta de presentación de un gerente de una empresa o de su representante legal.

No hay más casos de excepción adicionales para el principio de información, por lo que en cualquier circunstancia distinta a las antes descritas, el responsable estará obligado a poner a disposición de los titulares el aviso de privacidad.

3.1 Obligaciones ligadas al principio de información:

En resumen, de acuerdo con lo antes explicado, 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 LFDPPP, su Reglamento y los Lineamientos del Aviso de Privacidad, 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 directa o personal 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 el uso 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 (aprovechamiento), 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 y con una estructura y diseño que facilite su entendimiento, y atendiendo lo siguiente: no usar frases inexactas, ambiguas o vagas; tomar en cuenta los perfiles de los titulares; 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 en el Vigésimo de los Lineamientos del Aviso de Privacidad, con las características establecidas en los lineamientos Vigésimo primero a Trigésimo tercero;
11. Cuando se utilice la modalidad **simplificado** del aviso de privacidad, incluir todos los elementos informativos previstos en el Trigésimo cuarto al Trigésimo séptimo de los Lineamientos;
12. Cuando se utilice la modalidad **corto** del aviso de privacidad, incluir todos los elementos informativos previstos por el Trigésimo octavo al Cuadragésimo primero de los Lineamientos;

13. Utilizar la versión integral del aviso de privacidad cuando los datos personales sean obtenidos **personalmente** de los titulares;
14. Utilizar la versión simplificada del aviso de privacidad cuando los datos personales sean obtenidos **directamente** de los titulares. En este caso, el responsable podrá optar por poner a disposición de los titulares el aviso de privacidad integral, según lo considere conveniente;
15. Utilizar la versión corta del aviso de privacidad corto, únicamente cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de forma tal que los datos personales obtenidos también sean mínimos;
16. 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 o corta previo a la obtención o aprovechamiento de los datos personales;
17. No establecer cobros para la consulta del aviso de privacidad;
18. 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
19. 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.

3.2 ¿Cómo cumplo con el principio de información?

Obligación	Acciones recomendadas para el cumplimiento
	• Antes de elaborar el aviso de privacidad se recomienda: (i) identificar las actividades y procedimientos en los que utiliza datos personales; (ii) identificar cómo obtiene los datos personales; (iii) identificar el flujo de los datos personales al interior de la organización; (iv) identificar para qué fines se tratan los datos personales y qué tipo de datos se tratan para esas finalidades; (v) identificar las transferencias que se realizan; (vi) identificar los mecanismos que se ponen a disposición de los titulares para el

Obligación	Acciones recomendadas para el cumplimiento
	ejercicio de sus derechos, y (vii) identificar el perfil de los titulares. • Se recomienda utilizar el Generador de Avisos de Privacidad para elaborar el aviso de privacidad y de manera previa consultar la guía El ABC del Aviso de Privacidad. • Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.
Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera directa o personal del titular. 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. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso 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. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades (aprovechamiento), cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.	• Identificar de qué forma se obtienen los datos personales en cada actividad, tratamiento o procedimientos. • Establecer procedimientos y mecanismos para que el aviso de privacidad se ponga a disposición de los titulares en el momento en que lo indica la norma. • De manera particular, es importante llevar un control para no utilizar los datos personales si no se ha puesto a disposición de los titulares el aviso de privacidad, cuando éstos se obtienen de manera indirecta o cuando se van a tratar los datos para nuevas finalidades. • Capacitar al personal que recaba los datos personales, a fin de que conozca los momentos de la puesta a disposición del aviso de privacidad conforme a los supuestos aquí previstos.

Obligación	Acciones recomendadas para el cumplimiento
Redactar el aviso de privacidad de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento;	• Identificar el perfil de los titulares de los datos personales (por ejemplo, menores y personas en estado de interdicción o con discapacidad). • Si en el aviso de privacidad se incluyen ligas a sitios de Internet o documentos, revisar de manera frecuente que estas ligas estén habilitadas y funcionando de manera correcta, lo mismo para el caso de números telefónicos.
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.	• Verificar que el aviso de privacidad se coloque en un lugar con estas características.
Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales.	• Establecer procedimientos y mecanismos para que en las remisiones y transferencias de datos personales se proporcione a los encargados y terceros receptores de los datos, el aviso de privacidad correspondiente, y para que ello quede documentado y se pueda acreditar el cumplimiento de esta obligación.
Demostrar el cumplimiento del principio de información, en caso de que así se requiera.	• Generar pruebas para demostrar el cumplimiento del principio de información. • Cuando el instrumento para recabar el consentimiento expreso o expreso y por escrito sea el propio aviso de privacidad: conservar el aviso de privacidad con el consentimiento otorgado por el titular, para acreditar que obtuvo el consentimiento por parte del titular. • Cuando se requiera el consentimiento tácito: tener disponible el aviso de privacidad en las ventanillas donde se recaban los datos personales de los titulares, en el sitio de Internet del responsable, en carteles, o bien, la constancia de correos electrónicos donde se envía el aviso de privacidad, entre otras pruebas.
Cuando se utilice la modalidad integral del aviso de privacidad, incluir todos los elementos informativos previstos en el	• Consultar la guía El ABC del Aviso de Privacidad[3] y el Generador de Avisos de Privacidad (GAP),[4]

[3] http://abcavisosprivacidad.inai.org.mx/
[4] http://generador-avisos-privacidad.inai.org.mx/users/login

Obligación	Acciones recomendadas para el cumplimiento
Vigésimo de los Lineamientos del Aviso de Privacidad, con las características establecidas en los lineamientos Vigésimo primero a Trigésimo tercero. Cuando se utilice la modalidad simplificado del aviso de privacidad, incluir todos los elementos informativos previstos en el Trigésimo cuarto al Trigésimo séptimo de los Lineamientos. Cuando se utilice la modalidad corto del aviso de privacidad, incluir todos los elementos informativos previstos por el Trigésimo octavo al Cuadragésimo primero de los Lineamientos.	que el INAI pone a disposición de manera gratuita, a los responsables del tratamiento, con la finalidad de elaborar y actualizar los avisos de privacidad que correspondan a los tratamientos de datos personales que lleven a cabo, con plena observancia de todos y cada uno de los elementos informativos a que se refiere la LFPDPPP, su Reglamento y los Lineamientos.
Utilizar la versión integral del aviso de privacidad cuando los datos personales sean obtenidos personalmente de los titulares.	• Identificar las actividades, tratamientos o procedimientos en los que los datos personales se obtienen personalmente del titular. • Establecer los procedimientos y mecanismos necesarios para que se ponga a disposición de los titulares la versión integral del aviso de privacidad. • No es necesario que en cada formato en el que se obtienen los datos personales se incluya el aviso de privacidad integral, sino que éste se puede dar a conocer por ejemplo en carteles ubicados en las ventanillas en las que se obtienen los datos personales o en las pantallas de los ordenadores o tabletas. Lo importante en todo caso es que el aviso de privacidad esté ubicado en un lugar visible y de fácil consulta y que se dé a conocer a cada titular previo a la obtención de sus datos personales.
Utilizar la versión simplificada del aviso de privacidad cuando los datos personales sean obtenidos directamente de los titulares. En este caso, el responsable podrá optar por poner a disposición de los titulares el aviso de privacidad integral, según lo considere conveniente.	• Identificar las actividades, tratamientos o procedimientos en los que los datos personales se obtienen de manera directa del titular. • Establecer los procedimientos y mecanismos necesarios para que se ponga a disposición de los titulares, al menos, la versión simplificada del aviso de privacidad. En este caso, el responsable podrá optar por dar a conocer el aviso de

Obligación	Acciones recomendadas para el cumplimiento
	privacidad integral a los titulares. Sin embargo, se le sugiere tomar en cuenta el medio en que se difunde el aviso de privacidad, pues por citar un ejemplo, sería poco conveniente dar a conocer el aviso de privacidad integral vía telefónica. Es por ello que la LFPDPPP contempla la posibilidad de utilizar una versión simplificada del aviso de privacidad, a fin de hacer más eficiente su comunicación. • Algunas sugerencias según el medio en que se difunde el aviso de privacidad: (i) si se da a conocer a través del portal de Internet del responsable en razón de que por ese medio se obtienen los datos personales, se podría incluir una liga al aviso de privacidad antes de que el titular ingrese al formulario en el que proporcionará su información. Asimismo, el aviso de privacidad simplificado podría contener, a su vez, una liga para consultar el integral; (ii) si se da a conocer el aviso de privacidad por correo electrónico, en virtud de que por ese medio se solicitan datos personales, el aviso de privacidad se podría adjuntar al correo electrónico o bien incluir en el cuerpo del correo o una liga que conduzca al mismo; (iv) si el aviso de privacidad se da a conocer vía telefónica, se podría incluir una grabación que permita al titular conocer el aviso de privacidad previo a la obtención de sus datos personales, eligiendo una opción de marcado.
Utilizar la versión corta del aviso de privacidad corto, únicamente cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de forma tal que los datos personales obtenidos también sean mínimos.	• Utilizar esta modalidad de aviso, única y exclusivamente cuando sean pocos los datos personales que se recaban y el espacio para dar a conocer el aviso sea también reducido, como podría ser el caso de un boleto de rifa o un mensaje SMS.
Elaborar y tener disponible para su consulta el aviso de privacidad integral, con independencia de que se ponga a	• Verificar que el aviso de privacidad integral siempre esté disponible en el medio en que se está informando en el aviso de privacidad

Obligación	Acciones recomendadas para el cumplimiento
disposición de los titulares el aviso de privacidad en su versión simplificada o corta previo a la obtención o aprovechamiento de los datos personales.	simplificado o corto, para lo cual se recomienda hacer pruebas constantes en la liga de Internet, número telefónico o medio de que se trate.
No establecer cobros para la consulta del aviso de privacidad.	• Verificar que los medios en los que se difunde y pone a disposición el aviso de privacidad sean de acceso gratuito.
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. 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.	• Verificar con el área de tecnologías de la información o quien administra el portal de Internet del responsable si se utilizan estas tecnologías de rastreo, si a través de las mismas se obtienen datos personales y si se pueden deshabilitar y la forma para hacerlo. • Incluir en el portal de Internet el aviso que señala el artículo 14 del Reglamento de la LFPDPPP de forma tal que se pueda tener acceso al mismo desde el momento en que se ingresa al portal. • Establecer procedimientos a fin de que cuando se actualice alguno de los supuestos en mención se dé a conocer a cada titular el nuevo aviso de privacidad y se recabe su consentimiento, en su caso.

3.3 Lista de comprobación para el principio de información (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Cuenta con los avisos de privacidad necesarios, según los tratamientos que se realizan, para informar a los titulares sobre las características principales del tratamiento al que serán sometidos sus datos personales?			
2	Cuando recaba datos de forma personal o directa ¿da a conocer el aviso de privacidad previo a la obtención de los datos?			

3	Cuando obtiene datos de forma indirecta, ya sea a través de una transferencia o fuente de acceso público, y el tratamiento implica contacto con el titular ¿da a conocer el aviso de privacidad al primer contacto con éste?			
4	Cuando obtiene datos de forma indirecta, ya sea a través de una transferencia o fuente de acceso público, y el tratamiento no implica contacto con el titular, pero tiene datos para contactarlo ¿da a conocer el aviso de privacidad previo al aprovechamiento de los datos personales?			
5	Cuando hay cambio de finalidades ¿da a conocer el aviso de privacidad previo al aprovechamiento de los datos personales?			
6	¿Toma en cuenta el perfil de los titulares para la redacción del aviso de privacidad? ¿ha verificado que en el aviso de privacidad no se utilicen frases inexactas, ambiguas o vagas? ¿ha verificado que no se incluyan textos o formatos que induzcan al titular a elegir una opción en específico? ¿ha verificado que no se incluyan casillas pre-marcadas? ¿ha verificado que los textos a los que se remitan estén disponibles?			
7	¿El aviso de privacidad se encuentra ubicado en un lugar visible y de fácil consulta?			
8	¿Comunica el aviso de privacidad a encargados y terceros siempre que lleva a cabo una remisión o transferencia?			
9	¿Procura establecer mecanismos para generar evidencia de que se está cumpliendo con el principio de información?			
10	¿Se ha verificado que el aviso de privacidad en cualquiera de sus modalidades (integral, simplificado o corto) contenga todos los elementos informativos que exige la norma?			
11	¿Pone a disposición de los titulares el aviso de privacidad integral cuando los datos personales se obtienen de manera personal?			
12	¿Utiliza el aviso de privacidad simplificado sólo en los casos en que los datos personales se obtienen de manera directa?			
13	¿Utiliza el aviso de privacidad corto sólo en aquellos casos en los que los datos personales obtenidos son mínimos y el espacio para obtenerlos y dar a conocer el aviso es mínimo y limitado?			
14	¿Ha verificado que el aviso de privacidad integral esté disponible en el medio que se informó en el aviso de privacidad simplificado o corto?			
15	¿Los medios ofrecidos para consultar el aviso de privacidad son de acceso gratuito?			
16	Cuando así ocurre ¿informa en su portal de Internet sobre el uso de tecnologías de rastreo, que a través de éstas se obtienen datos personales y la forma en que se pueden deshabilitar?			
17	¿Pone a disposición de los titulares un nuevo aviso de privacidad en los supuestos en que así lo exige la norma?			
18	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de información?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con el principio de información.

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:

- Los Lineamientos del Aviso de Privacidad publicados en el DOF el 17 de enero de 2013 y disponibles en el portal de Internet del INAI en http://inicio.INAI.org.mx/MarcoNormativoDocumentos/Lineamientos_DOF.pdf
- La guía El ABC del Aviso de Privacidad, disponible en el portal de Internet del INAI en http://abcavisosprivacidad.inai.org.mx/, y
- El Generador de Avisos de Privacidad disponible en el portal de Internet del INAI en http://generador-avisos-privacidad.inai.org.mx/users/login

3.4 Medidas compensatorias

¿Qué son las 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 u otros mecanismos de amplio alcance, en lugar de poner a disposición el aviso a cada titular, de manera personal o directa. Lo anterior, siempre y cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados.

En ese sentido, los responsables pueden implementar medidas compensatorias para dar a conocer su aviso de privacidad a través de medios masivos de comunicación, y no de manera directa o personal a cada titular, cuando esto último resulte imposible o exija esfuerzos desproporcionados.

Se considera que existe una imposibilidad para dar a conocer el aviso de privacidad a cada titular, cuando el responsable no cuente con los datos personales necesarios que le permitan tener contacto 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.

Por otra parte, se considera que la puesta a disposición del aviso de privacidad a cada titular exige esfuerzos desproporcionados, cuando el número de titulares sea tal, que el hecho de poner a disposición de cada uno de ellos el aviso de privacidad, de manera personal o directa, implique al responsable un costo excesivo, al considerar su capacidad económica, así como el hecho de que se comprometa su estabilidad financiera, la realización de actividades propias de su negocio o la

viabilidad de su presupuesto programado; o bien, que dicha actividad sea disruptiva, de manera significativa, de aquéllas que el responsable lleva a cabo cotidianamente.

Ahora bien, para la implementación de medidas de compensatorias, el responsable requiere la autorización del INAI, la cual se puede obtener a través de dos vías:

1. Actualizando los supuestos previstos en los *Criterios Generales para la implementación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos*, publicados en el Diario Oficial de la Federación el 18 de abril de 2012, y
2. En caso de no actualizar estos supuestos, solicitando la autorización expresa del INAI.

Para conocer cuestiones básicas como cuándo se pueden instrumentar las medidas compensatorias; los supuestos en los que se requiere o no la autorización expresa del Instituto; los requisitos de presentación ante el INAI de una solicitud de autorización de medidas compensatorias; lugar y forma de presentar la solicitud; así como plazos para resolver la solicitud, se le invita a consultar la *Guía para instrumentar medidas compensatorias*, la cual se encuentra disponible a través del siguiente vínculo electrónico:
http://inicio.inai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf

4. 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 adquiere a través del servicio en línea de una tienda departamental, un reproductor de DVD y únicamente se solicitan los datos personales requeridos para su adquisición y envío a domicilio.
> X **Incorrecto:** Cuando se adquiere a través del servicio en línea de una tienda departamental, un reproductor de DVD, y si además de los datos personales para su adquisición y envío a domicilio se condiciona la compra a que el titular proporcione los lugares a los que el comprador piensa viajar, con la finalidad de enviarle publicidad, sin que esto tenga nada que ver con la compra que realizó el titular y sin que se le permita al mismo negarse para el tratamiento de sus datos para esta última finalidad.

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 estar previstas en el aviso de privacidad.

Con relación al tratamiento de **datos personales sensibles**, además de lo anterior, el responsable debe realizar esfuerzos razonables para **limitar el periodo** de tratamiento al mínimo indispensable. Asimismo, de acuerdo con el artículo 9 de la LFPDPPP, no podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades del responsable. En ese sentido, sólo podrán crearse bases de datos personales sensibles cuando:

1. Obedezca a un mandato legal;
2. Se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o
3. El responsable lo requiere para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

4.1 Obligaciones ligadas al principio de proporcionalidad:

En resumen, 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. Tratar el menor número posible de datos personales;
3. Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles, y
4. Crear bases de datos con datos personales sensibles sólo cuando (i) obedezca a un mandato legal; (ii) se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o (iii) el responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

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

4.2 ¿Cómo cumplo con el principio de proporcionalidad?

Obligación	Acciones recomendadas para el cumplimiento
Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.	• Identificar las finalidades del tratamiento de los datos personales y hacerse la pregunta ¿qué datos personales necesito para cumplir con esta finalidad? • Revisar los datos personales que se están tratando en cada una de las finalidades y, a partir de la respuesta dada en la pregunta anterior, hacerse la pregunta ¿son necesarios para cumplir con la finalidad? • Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.
Tratar el menor número posible de datos personales.	• A partir del análisis hecho anteriormente, realice un nuevo esfuerzo y trate de reducir al mínimo indispensable los datos personales que requiere para cumplir con las finalidades para las cuales se obtuvieron. • Elimine de sus bases de datos aquéllos que no son indispensables para cumplir con las finalidades, previo bloqueo, como se explicará más adelante en el principio de calidad.
Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.	• Verificar cuál es el periodo que se requieren conservar los datos personales sensibles, y una vez transcurrido el mismo, eliminar los datos,

	previo bloqueo, de acuerdo con lo que se explicará en el principio de calidad.
Crear bases de datos con datos personales sensibles sólo cuando (i) obedezca a un mandato legal; (ii) se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o (iii) el responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.	• Verificar que el tratamiento de datos personales sensibles atienda a alguno de los supuestos antes señalados.

4.3 Lista de comprobación para el principio de proporcionalidad (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Se asegura de que los datos personales que trata son necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron?			
2	¿Realiza esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios?			
3	En el caso de los datos personales sensibles ¿limita el periodo de tratamiento al mínimo necesario?			
4	Si trata datos personales sensibles ¿ha verificado que dicho tratamiento obedezca a alguno de los supuestos permitidos por la norma?			
5	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de proporcionalidad?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con el principio de proporcionalidad.

5. Principio de finalidad

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

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 determinada es cuando una tienda departamental, para prestar su servicio de compra en línea, señala que las finalidades del tratamiento de los datos personales que solicita son i) para verificar la identidad del cliente; ii) realizar el cobro respectivo, y iii) enviar el pedido solicitado a la dirección que el cliente proporciona.

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 darle la atención médica que solicita, realizarle los estudios y análisis que requiere, así como para el cobro y facturación de los servicios médicos.
> X **Incorrecto:** Sus datos personales serán tratados con la finalidad de darle la atención médica que solicita, realizarle los estudios y análisis que requiere, para el cobro y facturación de los servicios médicos, entre otros fines análogos.

¿Qué son las finalidades primarias y secundarias del tratamiento?
De acuerdo con el Reglamento de la LFPDPPP hay dos tipos de finalidades: (i) aquéllas que dan origen y son necesarias para la relación jurídica entre el titular y el responsable, a las cuales identificamos como **primarias**, y (ii) todas las demás que no cumplan con esta condición, a las que llamaremos **secundarias o accesorias**. Por ejemplo:

- Una persona proporciona sus datos personales a una universidad para que le preste un servicio educativo y, a su vez, la universidad desea utilizar estos datos para invitarla a los eventos anuales que realiza. En este caso, la finalidad primaria es la relacionada con la prestación del servicio educativo, en tanto que la finalidad secundaria o accesoria es la relacionada con la invitación a los eventos anuales.
- Una persona proporciona sus datos personales a una compañía de telecomunicaciones para que le preste el servicio de telefonía local y, a su vez, la compañía desea utilizar los datos de su cliente para promocionarle los servicios de televisión por cable e Internet. En este caso, la

[5] Ver apartado 3 Principio de Información, en donde se explica lo relativo al aviso de privacidad

finalidad primaria es la relacionada con la prestación del servicio de telefonía, en tanto que la finalidad secundaria o accesoria es la relacionada con la promoción de los servicios de televisión por cable e Internet.

Ahora bien ¿por qué el Reglamento de la LFPDPPP distingue entre finalidades primarias y secundarias? Esto ocurre porque, de acuerdo con el artículo 42 del Reglamento, **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 secundarias, sin que ello tenga como consecuencia la conclusión del tratamiento para las finalidades primarias.**

En ese sentido, se hace indispensable que en el aviso de privacidad se identifique y distinga entre las finalidades primarias y secundarias 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 secundarias. 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 secundarias.

¿Se pueden tratar los datos personales para finalidades distintas a las previstas en el aviso de privacidad?
Es importante que el responsable tome en consideración que no se pueden llevar a cabo tratamientos 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, a menos que:

- Lo permita de forma explícita una ley o reglamento, o
- El responsable haya obtenido el consentimiento para el nuevo tratamiento.

5.1 Obligaciones ligadas al principio de finalidad:

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

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 primarias y secundarias;
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 para finalidades secundarias;
6. No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias;
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.

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

5.2 ¿Cómo cumplo con el principio de finalidad?

Obligación	Acciones recomendadas para el cumplimiento
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.	• Establecer controles para evitar que los datos personales se traten para finalidades no previstas en el aviso de privacidad o que no hayan sido consentidas por el titular. • Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.
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.	• Identificar todas las finalidades para las cuales serán tratados los datos personales. • Incluir todas estas finalidades en el aviso de privacidad y redactarlas de forma tal que de manera clara, objetiva y sin lugar a confusión reflejen los objetivos del tratamiento. • Eliminar del aviso de privacidad todo tipo de frases que sean ambiguas o inexactas como: “entre otros”, “etcétera”, “de manera enunciativa más no limitativa”, “por

	mencionar algunos", "por ejemplo" u "otros fines análogos".
Identificar y distinguir en el aviso de privacidad entre las finalidades primarias y secundarias.	• Analizar las finalidades para las cuales se tratarán los datos personales y determinar cuáles de ellas son primarias y cuáles secundarias. • Redactar el aviso de privacidad de forma tal que se distinga con claridad qué finalidades son secundarias.
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.	• Desarrollar un mecanismo para que el titular pueda manifestar su negativa para el tratamiento de datos personales para finalidades secundarias. Este mecanismo debe permitir que se manifieste la negativa previo a que los datos personales sean tratados para dichas finalidades. En ese sentido, es conveniente que el mecanismo esté disponible al momento de recabar los datos y dar a conocer el aviso de privacidad. • Informar sobre la existencia de este mecanismo en el aviso de privacidad y la forma en que se puede hacer uso del mismo. • Considerar que el mecanismo puede ser el propio aviso de privacidad o cualquier otro que decida el responsable. Por ejemplo: • El aviso de privacidad puede ser adecuado cuando los datos se recaban por medio electrónico y por ese medio se da a conocer el aviso, ya que en este caso no es necesario reproducir en copia simple el aviso de privacidad a fin de recabar la manifestación de cada titular. En el aviso se podría incluir una casilla para que el titular manifieste, en su caso, su negativa. • Los registros o listados de exclusión, los números telefónicos o correos electrónicos son adecuados cuando el aviso de privacidad no se pone a disposición en medio electrónico, sino por ejemplo por

	teléfono o personalmente a través de un cartel. En estos casos es importante tener en cuenta que si el responsable ofrece un número telefónico o correo electrónico debe proporcionar al titular los medios para que en ese momento realice la llamada telefónica o envíe el correo respectivo.
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 para finalidades secundarias.	• Incluir la información relativa a este plazo en el aviso de privacidad. • Llevar un control con relación a la fecha en que se envió el aviso de privacidad y el término del plazo de cinco días hábiles. • No tratar los datos personales para estas finalidades antes de que concluya el plazo respectivo. • Si una vez concluido el plazo de cinco días e iniciado el tratamiento por parte del responsable, éste recibiera una negativa para el tratamiento por parte de un titular, se deberá concluir el tratamiento respectivo.
No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias.	• Establecer controles para evitar que lo anterior ocurra, y verificar que ningún procedimiento de la organización reproduzca esta práctica.
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.	• Establecer controles para evitar que los datos personales se traten para finalidades no previstas en el aviso de privacidad y que, en su caso, no hayan sido consentidas por el titular. • Establecer procedimientos para, en su caso, recabar el consentimiento del titular para las nuevas finalidades y dar a conocer el nuevo aviso de privacidad o la actualización del anterior, según sea el caso y lo explicado en la sección del principio de información.

5.3 Lista de comprobación para el principio de finalidad (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Las finalidades para las que se tratan los datos personales están previstas en el aviso de privacidad y, en su caso, fueron consentidas por el titular?			
2	¿Se incluyen en el aviso de privacidad todas las finalidades para las cuales se tratan los datos personales? ¿las finalidades son determinadas, es decir, claras, objetivas y que no den lugar a confusión?			
3	¿En el aviso de privacidad se distingue claramente las finalidades secundarias de las primarias?			
4	¿Tiene implementados mecanismos para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias? ¿se informa en el aviso de privacidad sobre esos mecanismos? ¿están disponibles para que el titular, en su caso, manifieste su negativa antes de que sus datos personales se traten para las finalidades secundarias?			
5	Cuando el aviso de privacidad se da a conocer a través de un medio indirecto, como el correo postal ¿informa al titular en el aviso de privacidad, que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias? ¿tiene implementado mecanismos para no tratar los datos personales antes de que concluya dicho periodo?			
6	¿Ha verificado que en sus procedimientos no se condicione el tratamiento para finalidades primarias, a que el titular consienta las finalidades secundarias?			
7	¿Solicita el consentimiento de los titulares para el tratamiento de sus datos personales para finalidades nuevas, que no fueron prevista de origen en el aviso de privacidad? O bien ¿ha verificado que alguna ley o reglamento permitan específicamente dicho tratamiento?			
8	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de finalidad?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con el principio de finalidad.

6. 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 son **exactos** cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. Por ejemplo, un dato no sería exacto si se registra en la base de datos que una persona cuenta con Doctorado en derecho, si el título que en realidad tiene es una Maestría en derecho.
- Los datos personales están **completos** cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular. Por ejemplo, los datos de salud del titular están completos cuando el expediente médico contiene todos los documentos clínicos e información que debe estar integrada al mismo.
- Los datos personales son **pertinentes** cuando corresponden efectivamente al titular. Por ejemplo, los datos del adeudo son pertinentes cuando corresponden al deudor y no a una homonimia.
- Los datos están **actualizados** cuando están al día y corresponden a la situación real del titular. Por ejemplo, el número telefónico que se tiene registrado en la base de datos está actualizado cuando, efectivamente, corresponde al titular con el que está vinculado.
- Los datos personales son **correctos** cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

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, pertinentes, correctos y actualizados cuando los proporciona directamente el titular, y hasta en tanto éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia que lo contradiga.

Datos obtenidos indirectamente

- En estos casos, se deben adoptar medidas razonables para que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, 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 aplicables en la materia de que se trate;
- Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y
- El periodo de bloqueo.

Entonces tenemos que:

$$\boldsymbol{Plazo\ de\ conservación} = Tiempo\ requerido\ para\ llevar\ a\ cabo\ las\ finalidades\ del\ tratamiento + plazos\ legales, administrativos, contables, fiscales, jurídicos\ e\ históricos\ aplicables + periodo\ de\ bloqueo.$$

En algunos casos estos tres tiempos o plazos pueden coincidir.

Por ejemplo: En la *NORMA Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico*, se señala en su apartado 5.4 que "[…] por tratarse de documentos elaborados en interés y beneficio del paciente,

deberán ser conservados por un periodo mínimo de 5 años, contados a partir de la fecha del último acto médico". En ese sentido, supongamos que una persona es paciente del Dr. Pérez por 10 años, entonces el Doctor tendría que conservar los datos personales contenidos en el expediente médico, por esos 10 años, más los cinco que establece la Norma, más el periodo de bloqueo (se explicará más adelante qué es el bloqueo), suponiendo que no hay plazos administrativos, contables, fiscales, jurídicos o históricos adicionales.

Ahora bien, es importante señalar que en particular, el artículo 11 de la LFPDPPP establece la obligación del responsable de eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contados a partir de la fecha en que se presente el mencionado incumplimiento.

¿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.

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

¡IMPORTANTE!
El responsable debe 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.

¿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 la supresión de los datos.

Siguiendo el ejemplo anterior, el Dr. Pérez tendría que bloquear los datos personales después de transcurrido los 15 años del tratamiento (10 años en que el titular fue su paciente + 5 años que establece la Norma). El tiempo en que los datos personales deberán estar bloqueados depende de los plazos legales o contractuales que existan 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.

6.1 Obligaciones ligadas al principio de calidad:

En resumen, de acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno al principio de calidad:

1. Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación;
2. Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;
3. Eliminar los datos personales relacionados con incumplimiento de obligaciones contractuales en un plazo de 72 meses, contados a partir de la fecha en que se presente el mencionado incumplimiento;
4. Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales;
5. Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación;
6. Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales, y
7. En caso 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.

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

6.2 ¿Cómo cumplo con el principio de calidad?

Obligación	Acciones recomendadas para el cumplimiento
Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello	• Establecer procedimientos para corregir y actualizar los datos personales no sólo en atención a solicitudes de ejercicio del derecho de rectificación, sino de oficio, cuando el responsable cuente con evidencia de que los datos en su posesión están incorrectos.

tenga como consecuencia que el titular se vea afectado por dicha situación.	• Realizar campañas de actualización de los datos personales, dirigidas a los titulares. • Informar a los encargados a los que se haya comunicados datos personales sobre las correcciones o actualizaciones de los datos personales que tengan lugar, a fin de que realicen lo conducente en la base de datos que manejen. • Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.
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.	• Verificar qué disposiciones normativas regulan la actividad en la que se tratan los datos personales, a fin de identificar si éstas imponen obligaciones de conservación de los datos personales por periodos específicos. • Verificar los plazos administrativos, contables, fiscales, jurídicos e históricos que resulten aplicables. • Verificar los plazos de prescripción legales y/o contractuales para fijar el periodo de bloqueo. • Definir el plazo de conservación a partir de lo anterior y establecer procedimientos para suprimir los datos personales concluido dicho periodo.
Eliminar los datos personales relacionados con incumplimiento de obligaciones contractuales en un plazo de 72 meses, contados a partir de la fecha en que se presente el mencionado incumplimiento.	• Verificar que no exista alguna disposición legal que disponga lo contrario. • En caso de que no la haya, establecer procedimientos para llevar un control de los plazos, a fin de suprimir los datos personales que procedan.
Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.	• Establecer el periodo de bloqueo según los plazos legales y contractuales que apliquen. • Establecer mecanismos y procedimientos para evitar que los datos personales se traten durante el periodo de bloqueo.

	• Llevar un control para suprimir los datos personales una vez que concluya el bloqueo.
Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación.	• Llevar un control para suprimir los datos personales una vez que concluya el plazo de conservación. • Establecer procedimientos seguros para la destrucción de los datos personales, que aseguren al máximo posible que los datos han sido eliminados de las bases de datos.
Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.	• Establecer por escrito los procedimientos para la conservación, bloqueo y supresión de los datos personales. • Incluir en los procedimientos los plazos de conservación, distinguiendo con claridad cuándo deberá empezar el periodo de bloqueo. Asimismo, detallar los pasos o fases para llevar a cabo el bloqueo y supresión de los datos personales.
En caso 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.	• Contar con el documento que establezca los procedimientos de conservación, bloqueo y supresión de los datos personales. • Elaborar bitácoras o cualquier otro documento en el que se acredite la fecha de bloqueo o supresión de los datos personales, y la información relevante con relación a dichas acciones.

6.3 Lista de comprobación del principio de calidad (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Ha adoptado medidas para procurar que los datos personales que trata sean exactos, completos, pertinentes, actualizados y correctos?			
2	¿Actualiza o corrige los datos personales cuando cuenta con evidencia objetiva que así lo justifique?			
3	¿Ha establecido el plazo de conservación de los datos personales? ¿considera en este plazo los tres elementos esenciales: (i) tiempo necesario para llevar a cabo las finalidades, (ii) cumplimiento de aspectos legales, administrativos, contables, fiscales, jurídicos e históricos, y (iii) periodo de bloqueo (plazos legales y contractuales para demostrar posibles responsabilidades)?			
4	En su caso ¿elimina los datos personales relacionados con incumplimiento de obligaciones contractuales en un plazo de 72 meses, contados a partir de la fecha en que se presente el mencionado incumplimiento?			

5	¿Bloquea los datos personales previo a su supresión, en el momento en que ello se requiere? ¿se asegura de que ninguna persona trate los datos personales que se encuentran en periodo de bloqueo?			
6	¿Se suprimen los datos personales una vez que concluyó el plazo de conservación? ¿tiene establecido procedimientos seguros para la eliminación de los datos personales?			
7	¿Tiene documentados los procedimientos de conservación, bloqueo y supresión de los datos personales?			
8	¿Cuenta con evidencia de que los datos personales se conservan, bloquean y suprimen atendiendo el principio de cancelación o en respuesta a una solicitud de ejercicio del derecho de cancelación?			
9	Cuando ello se requiere ¿informa a los encargados que manejan bases de datos a su nombre, sobre las modificaciones realizadas a los datos personales?			
10	¿Ha adoptado medidas que permitan verificar el cumplimiento del principio de calidad?			

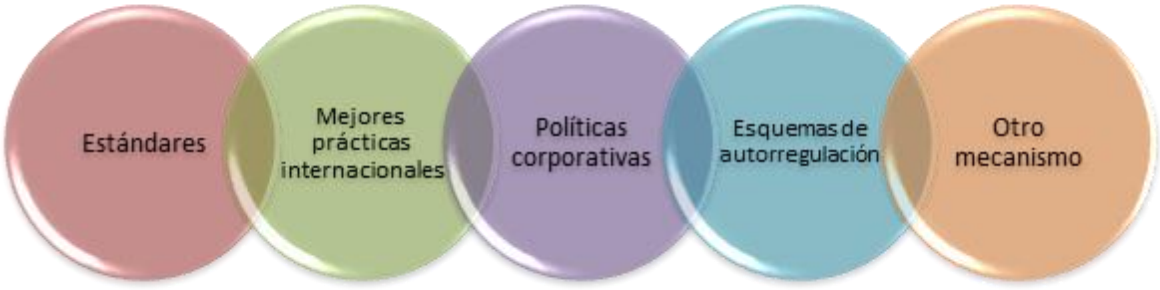
Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con el principio de calidad.

7. 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 se le conoce también como el principio de "rendición de cuentas", ya que 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 la autoridad, 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.

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



Por ejemplo, el responsable podría optar por desarrollar una política corporativa en materia 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 medidas se pueden adoptar para cumplir con el principio de responsabilidad?
Se debe tomar en cuenta que las medidas que adopte el responsable, además de garantizar el debido tratamiento, deben privilegiar los intereses del titular y su expectativa razonable de privacidad.

Ahora bien, entre las medidas que el responsable puede adoptar para cumplir con el principio de responsabilidad se encuentran, al menos, las siguientes:

I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;

II. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;

III. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;

IV. Destinar recursos para la instrumentación de los programas y políticas de privacidad;

V. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;

VI. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;

VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;

VIII. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;

IX. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento, o

X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

Es importante señalar que las medidas antes enlistadas no son las únicas que podría adoptar el responsable para cumplir con el principio de responsabilidad. Al contrario, el responsable 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.

7.1 Obligaciones ligadas al principio de responsabilidad

En resumen, de acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno al principio de responsabilidad:

1. Velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, aún por aquéllos comunicados a encargados;
2. Adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad, y
3. 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.

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

7.2 ¿Cómo cumplo con el principio de responsabilidad?

Obligación	Acciones recomendadas para el cumplimiento
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.	• Incluir en los contratos u otro instrumento jurídico que celebre con sus empleados, encargados y/o terceros, cláusulas en las que se comprometan a garantizar el adecuado tratamiento de los datos personales. • Establecer acciones técnicas y administrativas para la protección de los datos personales, tales como considerar el impacto a la privacidad en el diseño de sistemas de información, bases de datos y tratamiento. • Adoptar políticas de privacidad, adherirse a esquemas de autorregulación, hacer uso de estándares, mejores prácticas internacionales o mecanismos similares. • Establecer programas de capacitación y actualización, así como desarrollar contenidos que permitan concientizar a quienes tienen acceso a datos personales para el desarrollo de sus funciones. • Adoptar medidas que permitan supervisar, vigilar y verificar el grado de cumplimiento de la organización en materia de protección de datos personales, estableciendo también sanciones en caso de incumplimiento. • Analizar los riesgos que implica todo tratamiento de datos personales para el derecho fundamental a la protección de datos y la privacidad de sus titulares.
Tomar medidas para que los terceros con quienes mantiene una relación jurídica que implique el tratamiento de los datos personales,	• Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas en las que se establezca la

respeten el aviso de privacidad en el que se establezcan las condiciones de dicho tratamiento	obligación de realizar el tratamiento de los datos de conformidad con los términos señalados en el aviso de privacidad. • Documentar la comunicación del aviso de privacidad a terceros.

7.3 Lista de comprobación del principio de responsabilidad (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Tiene establecido procedimientos para verificar que se cumplan con los principios y obligaciones en materia de protección de datos personales, tanto al interior de su organización, como por parte de los encargados del tratamiento?			
2	¿Ha implementado alguna medida para garantizar el debido tratamiento y privilegiar los intereses y expectativa razonable de privacidad de los titulares, como por ejemplo políticas de privacidad, estándares, mejores prácticas, capacitación al personal, un sistema de supervisión y vigilancia del cumplimiento de la normativa en la materia, sanciones por incumplimiento, entre otros?			
3	¿Cuando comunica datos personales, celebra algún instrumento jurídico con el receptor de los datos, en el que conste que comunicó el aviso de privacidad y la obligación que tienen de realizar el tratamiento de acuerdo a lo establecido en dicho aviso? ¿verifica que los encargados realicen el tratamiento de conformidad con lo dispuesto en el aviso de privacidad?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con el principio de responsabilidad.

V. LOS DEBERES Y LAS OBLIGACIONES QUE CUMPLIR

Además de los ocho principios antes desarrollados y explicados, la protección de los datos personales se basa en dos deberes: el de confidencialidad y el de seguridad, los cuales se traducen también en obligaciones concretas para el responsable. A continuación se abordarán estos deberes.

A. Deber de Confidencialidad

Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Es por ello que 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 contractual, laboral o de otra naturaleza, entre el responsable del tratamiento y quien tenga acceso a los datos personales para el desarrollo de las tareas o funciones que se le hubieran encomendado.

Además, el responsable tiene que garantizar también que el deber de confidencialidad se cumpla incluso una vez finalizada la relación con el titular de los datos personales.

En definitiva, quienes traten datos personales, en cualquier fase del tratamiento, tienen que guardar secreto respecto de los datos que conozcan para el desarrollo de sus funciones.

A.1 Obligaciones ligadas al deber de confidencialidad

En resumen, de acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno al deber de confidencialidad:

1. Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con el titular, y
2. Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.

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

A.2 ¿Cómo cumplo con el deber de confidencialidad?

Obligación	Acciones recomendadas para el cumplimiento
Guardar confidencialidad de los datos personales, incluso después de finalizar la relación con el titular.	• Establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales. • Capacitar al personal para que conozca sus obligaciones con relación al tratamiento de datos personales.
Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.	• Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad. • Realizar verificaciones o supervisiones periódicas al trabajo realizado por los encargados, a fin de verificar que se cumplan con sus obligaciones en torno a la protección de los datos personales.

A.3 Lista de comprobación del deber de confidencialidad (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿Tiene implementadas medidas para garantizar la confidencialidad de los datos personales que trata?			
2	¿Se asegura de que sus empleados, encargados o terceros guarden confidencialidad respecto de los datos personales a los que tienen acceso?			
3	¿Prevé sanciones en caso de incumplimiento del deber de confidencialidad?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se esté cumpliendo cabalmente con el deber de confidencialidad.

B. Deber de Seguridad

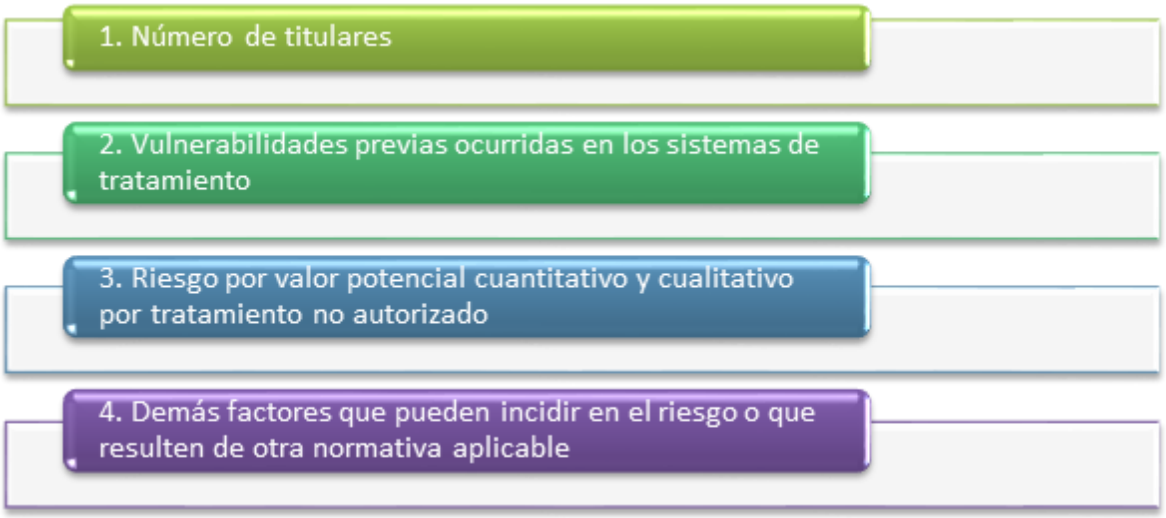
Este deber se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Las medidas adoptadas no podrán ser menores a aquéllas que los responsables y encargados tengan para el manejo de su información.

En ese sentido, el responsable deberá implementar las medidas de seguridad atendiendo lo que establece la LFPDPPP, su Reglamento y las disposiciones específicas que regulen el sector de la actividad que realice el responsable, siempre que éstas contemplen una protección mayor para el titular que las dispuestas en la LFPDPPP y su Reglamento.

¿Quién puede llevar a cabo las funciones de seguridad de los datos personales?
El responsable puede desarrollar y llevar a cabo las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.

¿Qué factores se deben tomar en cuenta para determinar las medidas de seguridad?
Las medidas de seguridad son el control o grupo de controles de seguridad destinados a la protección de los datos personales. Para determinar qué medidas de seguridad se deben implementar, el responsable deberá tomar en cuenta los siguientes factores:

De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:



¿Qué acciones se pueden llevar a cabo para la seguridad de los datos personales?
Para que el responsable pueda garantizar la seguridad de los datos personales, debe considerar las siguientes acciones, de acuerdo con lo dispuesto por el artículo 61 del Reglamento de la LFPDPPP:

I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
II. Determinar las funciones y obligaciones de las personas que traten datos personales;
III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;
V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
VII. Llevar a cabo revisiones o auditorías;
VIII. Capacitar al personal que efectúe el tratamiento, y
IX. Realizar un registro de los medios de almacenamiento de los datos personales.

El responsable debe contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.

¿Con qué frecuencia debo realizar actualizaciones a las medidas de seguridad?
Las actualizaciones a las medidas de seguridad que tenga implementadas el responsable, se realizarán cuando ocurran los siguientes eventos:

- Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable;
- Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo;
- Se vulneren los sistemas de tratamiento, o
- Exista una afectación a los datos personales distinta a las anteriores.

¡IMPORTANTE!
En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.

¿Qué se considera una vulneración a la seguridad?
Se consideran vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento, las siguientes:

¿Qué hacer en caso de una vulneración de seguridad?
El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

Para ello el responsable deberá informar al titular al menos lo siguiente:

- La naturaleza del incidente;

- Los datos personales comprometidos;
- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata, y
- Los medios donde puede obtener más información al respecto.

¿Qué hacer después de una vulneración de seguridad?
En caso de que ocurra una vulneración a los datos personales, el responsable, en primer lugar, debe analizar las causas por las cuales se presentó; y en segundo lugar, a efecto de evitar que la vulneración se repita, deberá implementar las acciones que a continuación se indican:

B.1 Obligaciones ligadas al deber de seguridad

En resumen, de acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno al deber de seguridad:

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas;
2. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su información;
3. Tomar en cuenta el riesgo inherente por tipo de dato personales; las posibles consecuencias para los titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico;
4. Considerar las acciones que establece el artículo 61 del Reglamento de la LFPDPPP pata la implementación y mantenimiento de las medidas de seguridad;
5. Actualizar las medidas de seguridad implementadas, cuando así se requiera, según los criterios antes descritos;
6. Notificar a los titulares las vulneraciones de seguridad que se presenten, con la información y en el momento antes señalados;
7. Llevar a cabo las acciones correctivas que sean necesarias.

B.2 ¿Cómo cumplo con el deber de seguridad?

El Instituto, en uso de sus atribuciones para emitir criterios y recomendaciones; divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, y proporcionar apoyo técnico a los responsables que lo soliciten, ha elaborado y puesto a disposición en su portal de Internet los siguientes materiales que orientan para el cumplimiento del deber de seguridad establecido en la LFPDPPP y su Reglamento:

1. Recomendaciones en materia de Seguridad de Datos Personales
Publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013. A través de éstas el Instituto sugiere la implementación de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), para la protección de los datos personales.

La adopción de las Recomendaciones es voluntaria, por lo que los responsables y encargados pueden decidir libremente qué metodología conviene más aplicar en su negocio para la seguridad de los datos personales, las cuales están disponibles en el siguiente vínculo: http://inicio.inai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf

2. Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales
Esta guía brinda orientación para la implementación del SGSDP, que se señala en las "Recomendaciones en materia de Seguridad de Datos Personales", el cual está basado en estándares internacionales. La guía se puede consultar en la siguiente liga: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

3. Metodología de Análisis de Riesgo BAA
En el marco de la emisión de las Recomendaciones en materia de Seguridad de Datos Personales, el INAI puso a consideración de los interesados, investigadores y expertos en materia de seguridad de la información, esa metodología para el análisis de riesgos en el entorno del tratamiento de datos personales, así como la selección de controles de seguridad a aplicar, la cual se encuentra disponible en:
http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

4. Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en Materia de Seguridad de Datos Personales
La Tabla de Equivalencia es un material de referencia para los responsables y encargados, que les permitirá evaluar si la implementación de determinados estándares internacionales en materia de seguridad de la información y privacidad en su organización facilitan el cumplimiento de los requisitos

y obligaciones que establece la LFPDPPP y su Reglamento en lo relativo a medidas de seguridad, así como las Recomendaciones en materia de Seguridad de Datos Personales. Esta herramienta puede ser consultada en:
http://inicio.ifai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf

5. Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas

El Manual tiene por objeto orientar a las micro, pequeñas y medianas empresas (MIPYMES), así como a organizaciones pequeñas, en el cumplimiento de las disposiciones establecidas en la Ley y su Reglamento, con relación a las medidas de seguridad para la protección de los datos personales, en este sentido el Manual es un documento de referencia para ayudar a los involucrados en el tratamiento de datos personales, en especial a aquellos grupos menos familiarizados con el tema de seguridad, a evaluar e implementar controles de seguridad sencillos en las actividades relacionadas con datos personales. El Manual puede ser consultado en:
http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf

Al ser una materia especializada, se recomienda consultar estos materiales para recibir orientación con relación a cómo cumplir con el deber de seguridad.

¡IMPORTANTE!
En los casos en que ocurra una vulneración a la seguridad de los datos personales, el Instituto, en su caso, podrá tomar en consideración el cumplimiento de sus recomendaciones, para efectos de determinar la atenuación de la sanción que corresponda.

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

Como se señaló en el glosario de esta guía, el encargado es quien trata los datos personales por cuenta del responsable. Esta figura tiene las siguientes características:

- Puede ser una persona física o moral;
- Puede ser del ámbito público o privado;
- Tiene que ser 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 en conjunto con otras personas;
- Se vincula con el responsable a través de una relación jurídica, que delimita el ámbito de su actuación, y
- No decide sobre el tratamiento de los datos sino que, en virtud de la relación jurídica que le vincula con el responsable, se limita a tratarlos por cuenta de este último, siguiendo sus instrucciones.

Por ejemplo: Si un hotel contrata a una empresa especializada en la elaboración y envío de facturas electrónicas, y por virtud de la prestación del servicio de facturación, el hotel le comunica los datos de sus clientes a dicha empresa para que les elabore la factura correspondiente por los servicios recibidos del hotel, en este supuesto estaríamos hablando de que la empresa que elabora las facturas 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.

¿Qué obligaciones debe establecer el responsable en su relación con el encargado?
De acuerdo con el artículo 50 del Reglamento de la LFPDPPP, el responsable deberá contemplar, al menos, las siguientes obligaciones del encargado en el instrumento jurídico en el que establezca la relación jurídica con éste:

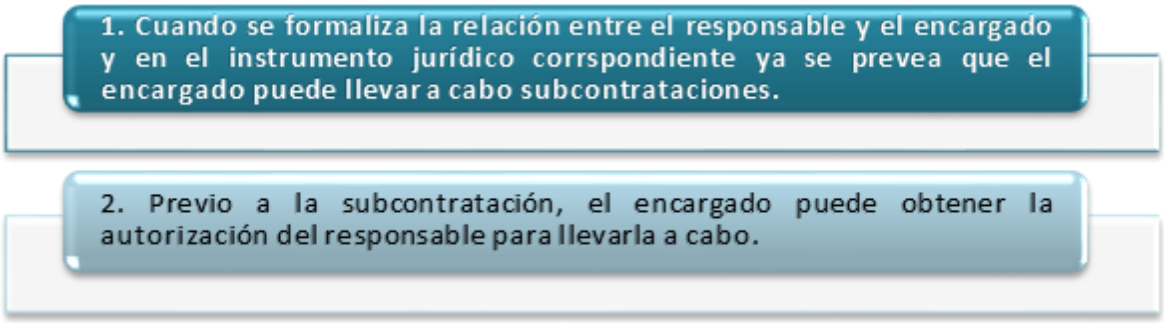
- Tratar únicamente los datos personales conforme a las instrucciones del responsable;
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- Implementar las medidas de seguridad conforme a la LFPDPPP, su Reglamento y las demás disposiciones aplicables;

- Guardar confidencialidad respecto de los datos personales tratados;
- Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
- Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

Asimismo, es importante señalar que cuando el encargado esté establecido en territorio mexicano estará obligado a establecer y mantener medidas de seguridad físicas, administrativas y técnicas según lo dispuesto por la LFPDPPP, su Reglamento y demás normatividad derivada.

¿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 empresas que le prestan algún servicio que implica el acceso a los datos personales del responsable. De acuerdo con el Reglamento de la LFPDPPP, el encargado puede llevar a cabo subcontrataciones, siempre que cuente con la autorización del responsable.

Hay dos momentos en los que se puede obtener la autorización de la subcontratación:



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 que implica el tratamiento de datos personales y este último hace uso de los servicios de otra persona física o moral para almacenar los datos personales en un servidor o en la nube, este último tratamiento de datos implica una subcontratación, que tendrá que estar autorizada por el responsable.

Corresponderá al encargado del tratamiento probar que tiene la autorización del responsable para subcontratar.

¿El encargado puede ser considerado responsable de los datos personales?
El encargado será considerado responsable de los datos personales, con las obligaciones propias de éste, cuando:

I. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o
II. Efectúe una transferencia, incumpliendo las instrucciones del responsable.

¿Qué pasa con el tratamiento de los datos personales en el servicio de cómputo en la nube?
Por cómputo en la nube se entiende el modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.

Cuando el responsable se adhiere a los servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, mediante condiciones o cláusulas generales de contratación, el proveedor de dichos servicios se constituye en encargado del tratamiento.

Ahora bien, de acuerdo con el artículo 52 del Reglamento de la LFPDPPP, para que el responsable se pueda adherir a un contrato para la prestación del servicio de cómputo en la nube, debe garantizar que el proveedor cumpla con las siguientes condiciones, pues de otra forma **NO PODRÁ** contratar dicho servicios:

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 LFPDPPP y su Reglamento;
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 presta 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 adecuadas 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:

En resumen, 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 su cuenta y nombre:

1. 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;
2. Fijar los acuerdos con el encargado con base en lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales;
3. Contemplar en el instrumento que establezca la relación jurídica con el encargado, al menos, las obligaciones que prevé el artículo 50 de la LFPDPPP;
4. Autorizar las subcontrataciones que realice el encargado, que involucren el tratamiento de datos personales;
5. Contratar servicios de cómputo en la nube que cumplan, al menos, con las condiciones descritas en el artículo 52 del Reglamento de la LFPDPPP, y
6. Verificar que el encargado cumpla con sus obligaciones.

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

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

Obligación	Acciones recomendadas para el cumplimiento
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.	• Diseñar cláusulas contractuales u otros instrumentos jurídicos en los que se establezcan los términos, condiciones y alcances del tratamiento de los datos personales por parte del encargado. • Se recomienda que estos instrumentos sean por escrito, para brindar certeza respecto de

	los acuerdos entre el responsable y encargado.
Fijar los acuerdos con el encargado con base en lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales.	• Tomar en cuenta los avisos de privacidad para fijar las obligaciones del encargado y los alcances y términos de la relación con éste. • Comunicar a los encargados los avisos de privacidad correspondientes.
Contemplar en el instrumento que establezca la relación jurídica con el encargado, al menos, las obligaciones previstas en el artículo 50 del Reglamento de la LFPDPPP. Autorizar las subcontrataciones que realice el encargado, que involucren el tratamiento de datos personales.	• No olvidar incluir en el instrumento que regule la relación con el encargado, las obligaciones previstas en el artículo 50 del Reglamento de la LFPDPPP. • Contemplar desde el inicio, es decir, desde que se celebre el instrumento jurídico en el que se establecen la relación con el encargado, la posibilidad o no de que éste pueda subcontratar servicios en los que se involucre el tratamiento de los datos personales. • En su caso, establecer por escrito que el encargado deberá solicitar la autorización del responsable para la subcontratación de servicios que impliquen el tratamiento de los datos personales.
Contratar servicios de cómputo en la nube que cumplan, al menos, con las condiciones descritas en el artículo 52 del Reglamento de la LFPDPPP.	• Revisar a detalle los contratos de adhesión para determinar si éstos cumplen con los requisitos establecidos en el artículo 52 del Reglamento de la LFPDPPP. • En su caso, realizar las consultas pertinentes al proveedor del servicio de cómputo en la nube, a fin de verificar que el servicio que ofrece cumpla con lo dispuesto por el artículo antes citado.
Verificar que el encargado cumpla con sus obligaciones.	• Realizar supervisiones o verificaciones eventuales al servicio prestado por el encargado, a fin de comprobar que esté cumpliendo con sus obligaciones en torno al tratamiento de datos personales. • Documentar cualquier incumplimiento. • Prever sanciones por los incumplimientos en la materia.

• En su caso presentar ante la autoridad las denuncias correspondientes.

iii. Lista de comprobación de la relación responsable-encargado (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	¿La relación con el encargado está establecida mediante un instrumento jurídico que permita comprobar su existencia, alcance y contenido?			
2	¿Los acuerdos con el encargado se basan en lo previsto en el aviso de privacidad en el que se definieron las condiciones del tratamiento?			
3	¿En el instrumento jurídico que se establecen las condiciones de la relación con el encargado se contemplan, al menos, las obligaciones del artículo 50 del Reglamento de la LFPDPPP?			
4	¿Ha quedado establecida la obligación del encargado de solicitar la autorización del responsable para realizar subcontrataciones que involucren el tratamiento de datos personales?			
5	¿Los servicios de cómputo en la nube que tiene contratados o que pretende contratar cumplen con los requisitos del artículo 52 del Reglamento de la LFPDPPP?			
6	¿Verifica que el encargado cumpla con sus obligaciones en torno a la protección de los datos personales?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se estén cumpliendo cabalmente las obligaciones en torno a la relación entre el responsable y el encargado.

En todo caso, es importante que el responsable tome en cuenta que, ante la ley y la autoridad, sigue respondiendo por los datos personales que estén siendo tratados por el encargado, por lo que debe ser de su mayor interés que éste cumpla con sus obligaciones.

VII. LAS TRANSFERENCIAS Y LAS OBLIGACIONES QUE CUMPLIR

La transferencia es la 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 consideran transferencia. A ese tipo de comunicaciones el Reglamento de la LFPDPPP 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 un hospital comunica los datos del paciente a su aseguradora, a fin de que se haga valer la cobertura del seguro para los gastos de hospitalización. Otro ejemplo sería cuando una empresa le transfiere datos a otra empresa del mismo grupo, a fin de que ésta última pueda ofrecer sus servicios al titular.

¿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 correspondiente lo siguiente: que la transferencia se podrá realizar, a quién se transferirán los datos y para qué fines. Asimismo, en caso de requerirse, el aviso de privacidad deberá contener una cláusula para que el titular consienta o no la transferencia;
2. El titular haya otorgado su consentimiento para que la transferencia se realice, salvo los casos de excepción previstos en el artículo 37 de la LFPDPPP, y
3. El objeto de la transferencia se deberá limitar a la finalidad y condiciones informadas en el aviso de privacidad, y que hayan sido consentidas por el titular, en su caso.

No se requerirá el consentimiento de los titulares para realizar transferencias, en los siguientes casos (artículo 37 de la LFPDPPP):

I. Cuando la transferencia esté prevista en una ley o tratado en los que México sea parte;
II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

Por otra parte, en el caso de las transferencias a las que refiere el inciso III anterior, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, el presente Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la LFPDPPP, su Reglamento y demás normativa aplicable.

¿Qué se requiere para llevar a cabo transferencias nacionales?

CONDICIÓN ESPECÍFICA	RECEPTOR DE LOS DATOS	FORMALIZACIÓN
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 finalidades consentidas e informadas.	El receptor de los datos personales adquirirá el carácter de responsable en términos de la LFPDPPP, 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?

CONDICIÓN ESPECÍFICA	RECEPTOR DE LOS DATOS	FORMALIZACIÓN
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.	El receptor de los datos personales NO podrá considerarse un responsable en términos de la LFPDPPP, pues al no estar establecido en territorio nacional, no le aplica la norma mexicana.	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

Asimismo, para que éstas ocurran será necesario 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 finalidades consentidas e informadas.	No obstante, mediante el instrumento jurídico de carácter privado en el que se establezca la relación con el responsable que transfiere los datos personales, deberá asumir las mismas obligaciones que éste tiene con relación al tratamiento de los datos personales. Si el tercero 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**.**	datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

Los responsables, en caso de considerarlo necesario, podrán solicitar la opinión del Instituto respecto a si las transferencias internacionales que realicen cumplen con lo dispuesto por la LFPDPPP y su Reglamento.

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

Para poder demostrar que la transferencia de datos personales, sea nacional o internacional, se realizó conforme a lo que establece la normativa en materia de protección de datos personales, la carga de la prueba recae tanto en el responsable que transfiere como en el receptor de los datos personales.

i. Obligaciones ligadas a las transferencias:

En resumen, de acuerdo con lo antes explicado, el responsable tiene las siguientes obligaciones en torno a las transferencias de datos personales:

1. Obtener el consentimiento del titular para las transferencias, salvo en el caso de que aplique algunas de las excepciones previstas en el artículo 37 de la LFPDPPP;
2. Informar las transferencias en el aviso de privacidad y, en su caso, incluir la cláusula correspondiente;

3. Limitar las transferencias a las finalidades y condiciones establecidas en el aviso de privacidad y que, en su caso, hayan sido consentidas por el titular;
4. Comunicar a los terceros receptores de los datos personales el aviso de privacidad, con las finalidades a las que el titular sujetó su tratamiento;
5. Demostrar que la trasferencia se hizo conforme a la normativa en materia de protección de datos personales;
6. Cuando la transferencia sea nacional, formalizarla mediante instrumento jurídico 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;
7. Cuando el responsable recibe los datos personales, tratarlo exclusivamente para las finalidades y bajo las condiciones informadas en el aviso de privacidad y, en su caso, consentidas por el titular;
8. Cuando se trate de transferencias internacionales, transferir los datos exclusivamente cuando el tercero receptor asuma las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, y
9. Cuando se trate de transferencias internacionales, formalizar la transferencia mediante instrumento jurídico que prevea 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 tratamiento de sus datos personales.

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

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

Obligación	Acciones recomendadas para el cumplimiento
Obtener el consentimiento del titular para las transferencias, salvo en el caso de que aplique algunas de las excepciones previstas en el artículo 37 de la Ley.	• Identificar las transferencias que se realizan en la organización del responsable. • Verificar e identificar para cuáles de las transferencias se requiere el consentimiento, a partir de los supuestos de excepción del artículo 37 de la Ley. • Implementar un mecanismo para solicitar el consentimiento del titular, en los casos que se requiera.
Informar las transferencias en el aviso de privacidad y, en su caso, incluir la cláusula correspondiente.	• Verificar que en el aviso de privacidad se informen todas las transferencias que se realizan, y para aquéllas que así lo

	requieran, se incluya la cláusula para que el titular las consienta. • Considerar que en caso de no requerir el consentimiento por encontrarse en alguno de los supuestos de excepción del artículo 37 de la Ley, ello no lo exime de la obligación de informar las transferencias en el aviso de privacidad.
Limitar las transferencias a las finalidades y condiciones establecidas en el aviso de privacidad y que, en su caso, hayan sido consentidas por el titular.	• Verificar los términos y condiciones planteados en el aviso de privacidad y establecer mecanismos para que las transferencias que se realicen sólo sean aquéllas previstas en el aviso.
Comunicar a los terceros receptores de los datos el aviso de privacidad, con las finalidades a las que el titular sujetó su tratamiento.	• Establecer mecanismos para que en todos los casos en que ocurran transferencias, se comunique al tercero receptor el aviso de privacidad correspondiente. • Conservar en soporte físico, electrónico o en cualquier otro formato, las comunicaciones que tenga con los terceros receptores, en los que conste que les hizo del conocimiento el aviso de privacidad.
Demostrar que la trasferencia se hizo conforme a la normativa en materia de protección de datos personales.	• Documentar los instrumentos jurídicos mediante los cuales se formalicen las transferencias.
Cuando la transferencia sea nacional, formalizarla mediante instrumento jurídico 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.	• Se sugiere utilizar un instrumento jurídico por escrito.
Cuando el responsable recibe los datos personales, tratarlo exclusivamente para las finalidades y bajo las condiciones informadas en el aviso de privacidad y, en su caso, consentidas por el titular.	• Exigir al responsable que transfiere los datos personales el aviso de privacidad correspondiente. • Implementar los mecanismos necesarios para que los datos personales se traten exclusivamente bajo las condiciones establecidas en el aviso de privacidad.

	• En caso de que el responsable receptor requiera tratar los datos personales para nuevas finalidades, informarlo al titular mediante el aviso de privacidad y, en su caso, solicitar su consentimiento.
Cuando se trate de transferencias internacionales, transferir los datos exclusivamente cuando el tercero receptor asuma las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales.	• En caso de que el tercero receptor no acepte esta condición, no realizar la transferencia.
Cuando se trate de transferencias internacionales, formalizar la transferencia mediante instrumento jurídico que prevea 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 tratamiento de sus datos personales.	• Incluir en el instrumento jurídico en el que se formalice la transferencia o se establezca la relación jurídica entre el responsable y el tercero receptor de los datos personales, la obligación de éste último de asumir las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales.

iii. Lista de comprobación de las transferencias (check-list)

No.	Pregunta	Respuesta		
		Sí	No	NA
1	Cuando no se actualiza alguna de las causales del artículo 37 de la LFPDPPP ¿solicita el consentimiento de los titulares para la transferencia?			
2	¿Informa en el aviso de privacidad que realiza transferencias, a quién y para qué finalidades?			
3	Cuando se requiere ¿incluye en el aviso de privacidad la cláusula para solicitar el consentimiento del titular?			
4	¿Realiza transferencias exclusivamente para las finalidades que establece el aviso de privacidad y a los terceros ahí señalados?			
5	¿Se asegura de comunicar a los terceros receptores el aviso de privacidad y las condiciones en las que el titular sujetó el tratamiento de sus datos personales?			
6	¿Cuenta con evidencia de que las transferencias se realizaron de acuerdo con lo que señala la norma?			
7	Cuando la transferencia es nacional ¿la formaliza mediante instrumento jurídico 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?			
8	Cuando usted es el responsable receptor de datos personales ¿utiliza los datos recibidos exclusivamente para los fines que se establecieron en el aviso de privacidad y que, en su caso, consintió el titular? O bien,			

	si desea tratar los datos para nuevas finalidades ¿solicita el consentimiento y pone a disposición del titular el aviso de privacidad?			
9	Cuando se trata de transferencias internacionales ¿transfiere los datos exclusivamente cuando el tercero receptor asume las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales?			
10	Cuando se trata de transferencias internacionales ¿las formaliza mediante instrumento jurídico que prevea 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 tratamiento de sus datos personales?			

Si en alguna de las preguntas la respuesta fue NO, será necesario realizar las acciones que correspondan, pues de lo contrario es probable que no se estén cumpliendo cabalmente las obligaciones en torno a las transferencias.

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

Incumplir con las obligaciones que tiene el responsable, implica vulnerar el derecho fundamental a la protección de datos personales del titular, y puede dar lugar a la imposición de una sanción económica si el Instituto verifica el incumplimiento.

El incumplimiento puede darse como consecuencia de una acción u omisión.

Además, el incumplimiento puede tener importantes implicaciones, tales como:

- Publicidad negativa, derivada de la falta de compromiso con el cumplimiento.
- Perder la confianza de:
  - Potenciales clientes o clientes y, por lo tanto, pérdida de negocio.
  - Inversores y/o accionistas.
- Imposibilidad de conseguir una certificación en protección de datos personales.

Tenga en consideración que la responsabilidad prevista en la LFPDPPP no sólo es administrativa, de manera que el incumplimiento puede dar lugar también a responsabilidad civil o penal, según corresponda.

En concreto, la LFPDPPP prevé las conductas que constituyen infracciones así como las sanciones que, en su caso, puede imponer el Instituto, ya que a éste le corresponde la potestad sancionadora.

¿Cuáles son las infracciones que prevé la Ley y qué sanciones me pueden imponer?
La siguiente tabla incluye las infracciones previstas en la Ley, el tipo de sanción aplicable en cada caso y la sanción correspondiente:

Infracción	Tipo de sanción	Sanción
No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la Ley.	No económica	Apercibimiento
Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales.	Económica	Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal[6]
Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable.		

[6] El salario mínimo vigente en el Distrito Federal se puede consultar en la siguiente dirección de Internet del Servicio de Administración Tributaria (SAT) http://www.sat.gob.mx/informacion_fiscal/tablas_indicadores/Paginas/salarios_minimos_2012.aspx o bien a través del sitio http://www.conasami.gob.mx/t_sal_mini_prof.html. / Dicho salario es establecido anualmente por la Comisión Nacional de Salarios Mínimos (http://www.conasami.gob.mx/) mediante resolución publicada en el Diario Oficial de la Federación.

Dar tratamiento a los datos personales en contravención a los principios establecidos en la Ley.		
Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de la Ley.		
Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.		
No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64 de la Ley.		
Incumplir el deber de confidencialidad establecido en el artículo 21 de la Ley.		Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal
Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12 de la Ley.		
Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.		
Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.		
Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley.		
Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.		
Obstruir los actos de verificación de la autoridad.		
Recabar datos en forma engañosa y fraudulenta.		
Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares.		
Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.		
Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de la Ley.		
Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la Ley.	—	—
Cuando de manera reiterada persistan las infracciones anteriores.	Económica	Multa adicional de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal
Infracciones cometidas en el tratamiento de datos sensibles.		Los montos podrán incrementarse hasta por dos veces

¿Hay responsabilidad penal en caso de que se cometa un delito?

Sin perjuicio de la responsabilidad administrativa que prevé la normatividad sobre protección de datos personales, podría ser exigible también responsabilidad penal o civil, en caso de que una acción u omisión dé lugar a la misma.

Por lo que se refiere a la responsabilidad penal, la LFPDPPP dedica su Capítulo XI, artículos 67 a 69, a los delitos en materia del tratamiento indebido de datos personales. Es así que se prevén los siguientes delitos y las sanciones que se indican en la siguiente tabla:

Materia/Cuestión	Acción	Elementos relevantes	Sanción
Medidas de seguridad	El que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.	• Ánimo de lucro	De tres meses a tres años de prisión.
Tratamiento de datos personales	Al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.	• Ánimo de lucro • Engaño	De seis meses a cinco años de prisión.
Datos personales sensibles	Las indicadas en los apartados anteriores.	Las indicadas en los apartados anteriores.	Se duplican.

Dicha responsabilidad penal será exigible, en su caso, ante las autoridades competentes.

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

Coordinación de Protección de Datos Personales

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
Insurgentes Sur No. 3211
Col. Insurgentes Cuicuilco, Delegación Coyoacán,
C.P. 04530

www.inai.org.mx