conalep

GUÍA DE PROTECCIÓN DE DATOS PERSONALES

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA
conalep

INICIO

Contenido

INICIO 2
Objetivo 4
Conceptos 4
Dato Personal 4
Dato Personal Sensible 4
Dato Personal Sensible 5
Titular 5
Responsable 5
Encargado 5
Transferencia de Datos Personales 6
Remisión de Datos Personales 6
DIAGNÓSTICO 7
¿Realizo tratamiento de Datos Personales? 7
¿Qué tipos de Datos Personales trato? 7
¿Cómo obtengo los Datos Personales? 7
¿Quiénes tratan los Datos Personales? 7
¿Para qué fines tratamos Datos Personales? 8
¿Transferimos o remitimos Datos Personales? 8
¿En dónde se resguardan los datos personales? 8
¿Por cuánto tiempo se resguardan los Datos Personales? 8
¿Cómo se suprimen los Datos Personales? 9
PRINCIPIOS 10
I. Principio de licitud 10
Obligaciones ligadas al principio de licitud: 10
¿Cómo cumplo con el principio de licitud? 10
II. Principio de lealtad 10
Obligaciones ligadas al principio de lealtad: 11
¿Cómo cumplo con el principio de lealtad? 11
III. Principio del consentimiento 11
Consentimiento Tácito 12
Consentimiento Expreso 12
Expreso y por escrito 12
Consentimiento cuando no hay contacto con el Titular 13

No es necesario el consentimiento 13
Cambio de las finalidades en el aviso de privacidad 14
¿Cómo demuestro que cumplí con el principio del consentimiento? 14
Obligaciones ligadas al principio de consentimiento 15
¿Cómo cumplo con el principio de consentimiento? 15
IV. Principio de información 16
¿Cuándo puedo hacer uso de cada una de las modalidades de aviso de privacidad? 18
Obligaciones ligadas al principio de información: 18
¿Cómo cumplo con el principio de información? 19
Medidas compensatorias 20
V. Principio de proporcionalidad 21
Obligaciones ligadas al principio de proporcionalidad: 21
¿Cómo cumplo con el principio de proporcionalidad? 21
VI. Principio de finalidad 21
¿Cómo cumplo con el principio de finalidad? 23
VII. Principio de calidad 23
VIII. Principio de responsabilidad 25
Obligaciones ligadas al principio de responsabilidad 26
¿Cómo cumplo con el principio de responsabilidad? 27
LOS DEBERES Y LAS OBLIGACIONES QUE CUMPLIR EN EL TRATAMIENTO DE DATOS PERSONALES 28
Deber de Confidencialidad 28
Deber de Seguridad 28
¿Qué factores se deben tomar en cuenta para determinar las medidas de seguridad? 30
¿Cómo implementar las acciones para la seguridad de los datos personales? 30
DOCUMENTO DE SEGURIDAD 36
¿Qué hacer en caso de una vulneración de seguridad? 36
¿A quién debo informar en caso de una vulneración? 36
EL EJERCICIO DE LOS DERECHOS ARCO 38
Procedimiento y plazos en una solicitud de ejercicio de derechos ARCO 42
La relación entre el responsable y el encargado y las obligaciones que cumplir 43
Las transferencias y las obligaciones que cumplir 46
Obligaciones ligadas a las transferencias: 48
Sanciones 50
Referencias 52

Objetivo

Facilitar el cumplimiento de las obligaciones en materia de protección de datos personales, mediante un material didáctico que sirva de consulta y apoyo para el cumplimiento de la normatividad en materia de Datos Personales.

Conceptos

Los conceptos básicos que se encuentran en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (Ley General), así como en los Lineamientos Generales de Protección de Datos Personales (Lineamientos) son:

Dato Personal

Es cualquier información concerniente a una persona física identificada o identificable, se considera que una persona es identificable cuando es posible reconocerla mediante los datos personales de que se traten.

Existen diferentes categorías de datos, por ejemplo:

DE IDENTIFICACIÓN: nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil, etc.
PATRIMONIALES: información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, etc.
ACADÉMICOS: trayectoria educativa, calificaciones, certificados, etc.

Dato Personal Sensible

Son aquellos datos personales que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave entre otros:

IDEOLÓGICOS: creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas.
DE SALUD: estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc.
CARACTERÍSTICAS PERSONALES: tipo de sangre, ADN, huella digital, hábitos sexuales, origen (étnico y racial.)
CARACTERÍSTICAS FÍSICAS: color de piel, iris y cabellos, señales particulares, etc., entre otros.

Tratamiento de Datos Personales

Tratar datos personales se refiere a cualquier operación u operaciones realizadas mediante procedimientos manuales o automatizados, relacionados con:

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

Titular

Es la persona física a quien refieren y pertenecen los datos personales que son objeto de tratamiento, aunque éstos estén en posesión de un tercero.

En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, se deberá dar cumplimiento a las reglas de representación dispuestas con las leyes civiles.

Responsable

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

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

Encargado

Es la persona física o jurídica, pública o privada, ajena al responsable, que trata los datos personales a nombre y por cuenta de este.

El encargado no decide sobre el tratamiento de los datos personales, sino que lo realiza siguiendo las instrucciones del responsable. Por ejemplo: la expedición de credenciales institucionales, que realiza un externo a esta (encargado), los datos que le son remitidos solamente podrá usarlos con esa finalidad; si tratara los datos personales para finalidades propias, de forma tal que decidiera sobre dicho tratamiento, se convertiría en un responsable, con todas sus obligaciones, y estaría sujeto a las sanciones previstas por la normativa correspondiente.

Transferencia de Datos Personales

Es toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

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

La transferencia de datos personales puede ser nacional o internacional, según el destino de los datos personales.

Ejemplo de transferencias:

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

Remisión de Datos Personales

Supone una comunicación de datos personales. La diferencia con la transferencia consiste en que, en la remisión, dicha comunicación se produce entre un responsable y un encargado del tratamiento.

Las remisiones también pueden ser nacionales o internacionales, sin importar que el responsable del tratamiento remita los datos personales a un encargado dentro o fuera del territorio nacional, el primero sigue siendo quien responde por el debido tratamiento de la información personal que comunicó.

Ejemplos de remisiones:

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

DIAGNÓSTICO

Para cumplir con las obligaciones en materia de Datos Personales, es importante identificar en los procesos internos que se realizan en cada unidad administrativa cómo se lleva a cabo el tratamiento de datos personales, para ello lo cual, se recomienda realizar un diagnóstico que permita identificar cuál es el flujo que, se sigue con respecto al tratamiento de los datos personales, desde que éstos se obtienen hasta que los mismos se eliminan.

Con la finalidad de facilitar la realización del diagnóstico se pueden contestar las siguientes preguntas:

¿Realizo tratamiento de Datos Personales?

En el marco de mis competencias y facultades para atender un trámite, para configurar una relación jurídica, en cumplimiento a una normatividad o cualquier otra actividad, solicito o trato uno o más Datos Personales.

¿Qué tipos de Datos Personales trato?

Se sugiere hacer un listado de TODOS los datos personales que se recaban y utilizan, haciendo la distinción de los datos personales sensibles.

¿Cómo obtengo los Datos Personales?

Los datos personales se pueden obtener de tres formas:

a) De forma personal. - Cuando el titular proporciona los datos personales mediante presencia física. Por ejemplo, cuando el titular acude a un hospital público (responsable) y ahí mismo proporciona sus datos personales.
b) De manera directa. - Cuando el titular proporciona los datos personales por algún medio que permite su entrega directa, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología. Por ejemplo, cuando el titular envía sus datos por correo electrónico o cuando los comunica vía telefónica.
c) De manera indirecta. - Cuando el responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, como podría ser a través de transferencias o fuentes de acceso público[1].

¿Quiénes tratan los Datos Personales?

Se deberán identificar las personas, áreas, departamentos o direcciones que realicen cualquier actividad relacionada con los Datos Personales que se captura en su Unidad

[1] 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.

Administrativa, así como identificar qué actividad en concreto realizan con los datos, por ejemplo, si los recaban y almacenan; si los recaban, transfieren o acceden a los mismos, etc.

¿Para qué fines tratamos Datos Personales?

Es necesario identificar cada una de las finalidades concretas para las cuales se tratan los datos personales, lo cual estar directamente relacionado con las actividades de la unidad administrativa en las cuales se utilizan datos personales, por ejemplo, nómina o expediente en el caso de la Dirección de Personal, o con tramites o servicios que se realizan en el Colegio.

¿Transferimos o remitimos Datos Personales?

Si comunicamos datos a encargados, para que estos traten los datos a nombre y por cuenta del Colegio, a esta comunicación de datos personales se le denomina remisión. La relación entre ambos deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que se decida como responsables de los datos y de conformidad con la normativa aplicable.

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

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

¿En dónde se resguardan los datos personales?

Los datos personales que trata pueden estar almacenados en:

Soporte electrónico: En dispositivos electrónicos, equipos de cómputo, etc.
Soporte físico: Archivos físicos, archiveros, almacenes etc.

¿Por cuánto tiempo se resguardan los Datos Personales?

Los sujetos obligados, de conformidad con lo establecido en la Ley General de Archivos, deben determinar a través de un análisis de procesos y procedimientos: la vigencia de los documentos, plazos de conservación y el catálogo de disposición documental[2]. Se deben considerar las disposiciones específicas para la conservación y destrucción de la información.

[2] Título Tercero de la Valoración y Conservación de los Archivos, Capítulo I de la Valoración, así como artículo 36, ambos de la Ley General de Archivos

¿Cómo se suprimen los Datos Personales?

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

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

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

PRINCIPIOS

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:

I. Principio de licitud

Los datos personales tienen que ser tratados de manera lícita, lo que supone que se debe estar sujeto a las facultades o atribuciones que la normatividad aplicable otorga al responsable, es decir, sólo podrá hacer con los datos personales aquello que esté legalmente permitido, como cualquier acto de autoridad, por lo que, no deben tratarse datos personales si no se tienen facultades previamente otorgadas.

Obligaciones ligadas al principio de licitud:

Las obligaciones derivadas del principio de licitud son:

1) Tratar siempre los datos personales de conformidad con las atribuciones o facultades conferidas por la normatividad mexicana y, en su caso, el derecho internacional.
2) El tratamiento se debe realizar tomando en consideración los derechos y libertades de los titulares y respetando la garantía de legalidad de los gobernados.

¿Cómo cumplo con el principio de licitud?

Identificando el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, manuales, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales para cada una de las finalidades, y aquél que regula el tratamiento respectivo.

II. Principio de lealtad

Este principio determina que, la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

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

Con este principio no se permite el tratamiento, tramposo, deshonesto y no ético de la información sobre los titulares.

Obligaciones ligadas al principio de lealtad:

Se tienen las siguientes obligaciones en torno al principio de lealtad:

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

¿Cómo cumplo con el principio de lealtad?

1. Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.
2. Verificar continuamente los tratamientos que se realizan, a fin de confirmar que no den lugar a discriminación o trato injusto o arbitrario en contra del titular.
3. Elaborar avisos de privacidad con todos los elementos informativos que establece la Ley General, y con información que corresponda a la realidad del tratamiento que se efectúa.
4. Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto.
5. Llevar a cabo el tratamiento de los datos personales sólo para los fines informados en el aviso de privacidad.

III. Principio del consentimiento

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

- ✓ Correcto: solicitar el consentimiento para el envío de información relacionada con nuevos trámites sobre servicios que realiza el sujeto obligado.

- ✗ Incorrecto: solicitar el consentimiento para el uso de los datos personales en general, para cualquier finalidad que se le ocurra al responsable en el futuro. Por ejemplo: mencionar en el aviso de privacidad, sus datos personales serán recabados para las finalidades mencionadas y cualquier otra que se requiera.

El consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad, el consentimiento debe ser libre, en el sentido que no medie error, mala fe, violencia o dolo que puedan afectar la voluntad del titular.

¿Cómo se obtiene el consentimiento?

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

Consentimiento Tácito
Se requiere para cualquier tipo de dato personal, con excepción de los considerados como sensibles.

El consentimiento tácito se obtiene si el titular no se niega a que sus datos personales sean tratados, después de haber conocido el aviso de privacidad. Es decir, no es necesario que quede registrado que el titular autorizó el tratamiento de su información personal, sino que es suficiente con que no se niegue al tratamiento.

Por ejemplo, el consentimiento tácito podría solicitarse a través de la siguiente frase:

> En caso de que no desee que sus datos personales sean tratados para las finalidades antes descritas, indíquelo a continuación;
>
> ▫ No consiento que mis datos personales sean tratados para las finalidades antes descritas.

Si el titular no indicara en el recuadro, que no consiente el tratamiento de sus datos personales, el responsable podría suponer que tiene el consentimiento para el tratamiento, siendo suficiente con que no diga que no

Consentimiento Expreso
Para cualquier tipo de dato personales, con excepción de los datos personales sensibles.

Este tipo de consentimiento deberá expresarse de las siguientes maneras: Verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología.

Deberá implementarse un medio sencillo para manifestar la voluntad, por ejemplo:

> ▫ En caso de estar de acuerdo con recibir información, podrá manifestarlo señalando la casilla con X

Expreso y por escrito
Se requiere para datos personales sensibles.

El consentimiento se deberá otorgar por escrito, mediante firma autógrafa, huella dactilar, firma electrónica del titular o cualquier otro mecanismo autorizado que permita identificarlo plenamente, el cual podrá ser físico o electrónico.

Por ejemplo:

> En caso de estar de acuerdo con las finalidades para las cuales se recaban sus datos personales sensibles, señale:
>
> _____
> Nombre y Firma

Si una ley o reglamento, en lo particular, exige el consentimiento expreso o expreso y por escrito para el tratamiento, se deberá solicitar de esa forma, aunque no se trate de datos sensibles.

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.

El consentimiento deberá ser expreso y por escrito, cuando no se actualice alguno de los supuestos de excepción para recabar el consentimiento previstos en el artículo 22 de la Ley General.

Consentimiento cuando no hay contacto con el Titular

De acuerdo con lo señalado por el segundo párrafo del artículo 15 de los Lineamientos Generales, en caso de que no se 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, como podría ser a través de una transferencia o fuente de acceso público.
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.

Es posible asumir que cuenta con el consentimiento tácito 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, lo cual se deberá informar en el aviso de privacidad especificando claramente que, el titular cuenta con cinco días hábiles para manifestar su negativa para el tratamiento de su información y aquellas finalidades que requieren el consentimiento tácito.

Cuando se requiera el consentimiento expreso o expreso y por escrito, necesariamente tendrá que contactar personal o directamente al titular para obtenerlo, así como documentar la puesta a disposición del aviso de privacidad.

No es necesario el consentimiento

No es necesario obtener el consentimiento, cuando ocurra alguno de los siguientes supuestos:

- Cuando una ley así lo disponga.
- Cuando las transferencias se realicen entre responsables, se trate de datos personales que utilicen en el ejercicio de las facultades del responsable o, sean compatibles o análogas con la finalidad que dio origen al tratamiento.
- Cuando exista una orden judicial, resolución o mandato.
- Para el reconocimiento o defensa de derechos del titular ante alguna autoridad.
- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
- Cuando exista una situación de emergencia que pueda dañar a un individuo en su persona o sus bienes.
- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria.
- Cuando los datos personales figuren en fuentes de acceso público.
- Cuando los datos personales se sometan a un procedimiento previo de disociación[3].
- Cuando el titular de los datos sea una persona reportada como desaparecida.

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.

Cambio de las finalidades en el aviso de privacidad

En caso de cambiar las finalidades establecidas en el aviso de privacidad, será necesario solicitar, mediante un nuevo aviso, la información relativa a las nuevas finalidades, el consentimiento de los titulares para las nuevas finalidades, siempre y cuando estas no actualicen los supuestos de excepción antes mencionados.

¿Cómo demuestro que cumplí con el principio del consentimiento?

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 o la constancia de correos electrónicos donde se envía el aviso de privacidad.

[3] **Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de este.

Obligaciones ligadas al principio de consentimiento

Se tienen las siguientes obligaciones en torno al principio de consentimiento:

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

¿Cómo cumplo con el principio de consentimiento?

1. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.
2. En esos casos, solicitar el consentimiento de los titulares conforme se requieran.
3. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.
4. Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales.
5. Definir el tipo de consentimiento que se requiere, según el tipo de datos personales.
6. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso y documentar su obtención.
7. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.
8. Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.

9. Cuando los datos personales no los proporcione personal o directamente el titular, se deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa.
10. En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte.
11. Prever en el procedimiento interno para la atención de solicitudes de derechos ARCO lo relativo a la revocación del consentimiento, según los plazos, requisitos y procedimiento que se establecen para el ejercicio de los derechos de cancelación y oposición.

IV. Principio de información

Por virtud de este principio, se tiene la obligación de informar a los titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad.

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 en las diversas actividades que realicen dentro de sus funciones, es decir no puede haber un aviso de privacidad genérico para todos los datos que se tratan en el Colegio.

La puesta a disposición del aviso de privacidad implica publicar en un lugar visible, accesible y gratuito, no obstante, el CONALEP no está obligado a entregar una copia del aviso de privacidad al titular, a menos que éste lo solicite.

Se sugiere hacer uso del Generador de Avisos de Privacidad (GAP) Sector Público, que es una herramienta informática gratuita, creada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), para facilitar la creación de avisos de privacidad.

Este aviso podrá difundirse, ponerse a disposición o reproducir en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación; en todo caso, deberá estar ubicado en un lugar visible y que facilite su consulta.

Esto último también tiene como finalidad acreditar ante el INAI el cumplimiento de su obligación.

Modalidades

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

Elementos del aviso de privacidad en cada una de las modalidades

ELEMENTO INFORMATIVO	INTEGRAL	SIMPLIFICADO
1. Denominación del responsable.	✓	✓
1bis (opcional). Abreviatura o acrónimo por el cual se identifica al responsable.	✓	✓
2. Domicilio del responsable.	✓	
2bis (opcional). Datos de contacto.	✓	
3. Datos personales.	✓	
3bis (opcional). Medios y/o fuentes de obtención de los datos personales.	✓	
4. Finalidades del tratamiento.	✓	✓
5. Transferencias que requieren consentimiento	✓	✓
5bis (opcional). Transferencias que no requieren el consentimiento.	✓	
6. Negativa del consentimiento.	✓	✓
7. Sitio donde se podrá consultar el aviso de privacidad integral.	✓	
8. Fundamento legal.	✓	
9. Derechos ARCO y Portabilidad.	✓	
10. Portabilidad	✓	
11. Domicilio de la Unidad de Transparencia.	✓	
12. Cambios al aviso de privacidad.	✓	
13. Fecha de elaboración o última actualización.	✓	✓
14. Características del aviso de privacidad	✓	✓

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

Aviso de Privacidad Simplificado: El responsable deberá poner a disposición del titular el aviso de privacidad simplificado en un primer momento.

Aviso de Privacidad Integral: El aviso de privacidad integral deberá estar publicado, de manera permanente, en el sitio o medio que se informe en el aviso de privacidad simplificado.

Lo anterior no implica que en su modalidad integral no pueda ponerse a disposición del titular en un primer momento.

Los responsables del tratamiento de los datos 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 normatividad a través de los medios que estime pertinentes, como, por ejemplo, fotografías, grabaciones telefónicas, fe de hechos o firmas de los titulares, entre otros.

Obligaciones ligadas al principio de información:

Las obligaciones en torno al principio de información son las siguientes:

1. Poner a disposición de los titulares el aviso de privacidad en los términos que fije la Ley General en la materia y sus Lineamientos, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales.
2. Poner a disposición el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera personal y directa del titular.
3. Poner a disposición del titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, que no requiera el consentimiento, o bien de una fuente de acceso público.
4. Poner a disposición del titular el aviso de privacidad previo a iniciar tratamiento de los datos personales para la finalidad para la que se obtuvieron (aprovechamiento), cuando éstos no se hayan obtenido de manera directa del titular, el tratamiento no requiera del contacto con él y se cuente con datos para contactarlo.
5. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades, cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.
6. Redactar el aviso de privacidad de manera que sea claro, comprensible, con una estructura y diseño que facilite su entendimiento, para su elaboración tomar en cuenta el perfil de los titulares y atender lo siguiente: no usar frases inexactas, ambiguas o vagas; incluir textos o formatos que induzcan al titular a elegir una opción en específico; no pre-marcar casillas en las que se solicite el consentimiento del titular, y no remitir a textos o documentos que no estén disponibles.

7. Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.
8. Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales.
9. Demostrar el cumplimiento del principio de información, en caso de que así se requiera.
10. Cuando se utilice la modalidad integral del aviso de privacidad, incluir todos los elementos informativos previstos de la normatividad aplicable.
11. Cuando se utilice la modalidad simplificada del aviso de privacidad, incluir todos los elementos informativos correspondientes.
12. Elaborar y tener disponible para su consulta el aviso de privacidad integral, con independencia de que se ponga a disposición de los titulares el aviso de privacidad en su versión simplificada previo a la obtención o aprovechamiento de los datos personales.
13. No establecer cobros para la consulta del aviso de privacidad.
14. En caso de que se utilicen tecnologías de rastreo, esto se debe informar en el Portal CONALEP, 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 a través de éstas se pueden recabar datos personales y la forma en cómo se pueden deshabilitar.
15. Poner a disposición de los titulares un nuevo aviso de privacidad en los siguientes casos:
    a. Cambie la identidad del responsable (CONALEP).
    b. Se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular.
    c. Se requiera tratar los datos personales para nuevas finalidades que requieran el consentimiento del titular.
    d. Se requiera realizar nuevas transferencias que requieran el consentimiento del titular.

¿Cómo cumplo con el principio de información?

El cumplimiento de este principio está relacionado con una clara y correcta redacción de los dos tipos de aviso de privacidad, así como su presentación al titular de los datos en los momentos que se han señalado y que están determinados por la normatividad en materia de Datos Personales.

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 de comunicación masiva en lugar de hacerlo de manera personal o directa. Lo anterior, siempre y cuando resulte imposible dar a conocer el aviso de privacidad al titular de manera directa o exija esfuerzos desproporcionados.

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

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

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

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

Se deberán publicar los avisos de privacidad simplificados en la instrumentación de medidas compensatorias en:

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

V. 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: Solicitar exclusivamente los datos personales que la legislación aplicable manifiesta para el trámite correspondiente.

Incorrecto: Solicitar requisitos adicionales no estipulados en la normatividad y estos, contengan datos personales.

Se deben, como responsables de los Datos Personales, realizar esfuerzos razonables para que sean solicitados los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron.

Obligaciones ligadas al principio de proporcionalidad:

Se tiene las siguientes obligaciones en torno al principio de proporcionalidad:

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

¿Cómo cumplo con el principio de proporcionalidad?

Actividades para su cumplimiento:

1. Identificar qué datos personales se requieren para cada una de las finalidades. El listado de datos personales debe estar completo con independencia de que en el aviso de privacidad se informe por categoría de datos.
2. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.
3. Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.
4. Requerir el mínimo posible de datos personales para lograr las finalidades para las cuales se tratan.

VI. Principio de finalidad

Es el propósito, motivo o razón por el cual se tratan los datos personales.

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

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

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

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

Por ejemplo:

Correcto: Sus datos personales serán tratados con la finalidad de contribuir en la generación de información estadística en colaboración con el INEGI.

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

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

Solo se podrán tatar datos personales que no hayan sido informados previamente al titular en los siguientes supuestos:

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

Obligaciones ligadas al principio de finalidad:

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

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.
2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas.
3. Identificar y distinguir en el aviso de privacidad entre las finalidades que dan origen al tratamiento de aquellas que son distintas a las que lo originaron, pero se consideran compatibles y/o análogas.
4. Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias.
5. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como el correo postal, informar al titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información.
6. No condicionar el tratamiento para finalidades, con aquellas distintas a las que dieron origen al tratamiento.
7. Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento del titular de los datos.

¿Cómo cumplo con el principio de finalidad?

Actividades para su cumplimiento

1) Identificar las finalidades de cada tratamiento que se realice, verificar que atiendan a fines específicos o determinados y que sean acordes a las atribuciones o facultades del Colegio y de la unidad administrativa de que se trate.
2) Verificar que en los avisos de privacidad se informan todas las finalidades para las cuales se tratan los datos personales, y que se describen de manera clara.
3) Identificar qué finalidades requieren consentimiento y solicitarlo según las reglas descritas anteriormente.
4) Identificar el marco normativo que otorga las atribuciones a la unidad administrativa para tratar los datos personales para cada una de las finalidades.
5) Identificar las finalidades que no fueron informadas en los avisos de privacidad y que se requieran llevar a cabo.
6) Solicitar el consentimiento de los titulares para el tratamiento de datos personales para estas finalidades adicionales, cuando el mismo se requiera.

VII. 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:

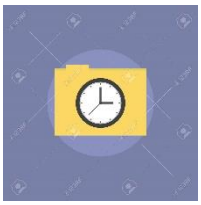
Exactos y correctos: Cuando en posesión del responsable no presentan errores que pudieran afectar su veracidad.
Completos: Cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.
Actualizados: Cuando los datos personales responden fielmente a la situación actual del titular.

Se deben 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.

¿Cuánto tiempo puedo conservar los datos personales?

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

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



El artículo 24 la Ley General, establece que se deben documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales respecto de cada tratamiento que se efectúe.

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

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

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

Por ejemplo, Se tendría que bloquear los datos personales después de transcurrido los 15 años del tratamiento (10 años en que el titular tuvo una relación con la institución + 5 años que establecía la norma). El tiempo en que los datos personales deberán estar bloqueados depende de los plazos legales que establezca la legislación de índole archivística, 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.

Obligaciones ligadas al principio de calidad:

Las obligaciones en torno al principio de calidad son:

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

¿Cómo cumplo con el principio de calidad?

Actividades para su cumplimiento:

1) Implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completen, en las distintas bases de datos que estén a cargo de la unidad administrativa.
2) Permitir que la modificación de los datos personales sea inmediata, una vez que la unidad administrativa tenga conocimiento de la actualización o corrección a que haya lugar.
3) Establecer los plazos de conservación de los datos personales, para cada uno de los tratamientos, lo cual deberá ser congruente con los plazos de conservación establecidos en los instrumentos de clasificación archivística.
4) Elaborar los procedimientos para la conservación y supresión de los datos personales, así como documentarlos. Estos procedimientos podrán ser los establecidos en materia de archivos, si a través de estos se puede cumplir con la obligación prevista en la Ley General.

VIII. Principio de responsabilidad

Este principio establece la obligación de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y los órganos garantes, que cumple con sus obligaciones en torno a la protección de los datos personales, aun y cuando los datos estén siendo tratados por encargados.

Este principio supone que el responsable tome las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica, así como al momento de realizar transferencias nacionales o internacionales de datos personales.

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

- Estándares
- Mejores prácticas nacionales e internacionales

¿Qué mecanismos se pueden adoptar para cumplir con el principio de responsabilidad?
Se debe tomar en cuenta que los mecanismos que se adopten, además de garantizar el debido tratamiento, deben privilegiar los intereses del titular y su expectativa razonable de privacidad, los cuales se encuentran señalados en el artículo 30 de la Ley General que establece lo siguiente:

1) Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales.
2) Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles.
3) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
4) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
5) Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
6) Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
7) Diseñar, desarrollar e implementar políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley General y las demás que resulten aplicables en la materia.
8) Garantizar que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley.

Obligaciones ligadas al principio de responsabilidad

Estas son las obligaciones en torno al principio de responsabilidad:

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

¿Cómo cumplo con el principio de responsabilidad?

Actividades para su cumplimiento:

1. Prever presupuesto para la instrumentación de programas y políticas de protección de datos personales.
2. Elaborar un programa de protección de datos personales que contemple el cumplimiento obligatorio.
3. Elaborar y aplicar un programa de capacitación y actualización de los servidores públicos en materia de protección de datos personales.
4. Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad.
5. Establecer un procedimiento para atender dudas y quejas de los titulares con las características señaladas en la columna anterior.
6. En todos los casos generar pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.

LOS DEBERES Y LAS OBLIGACIONES QUE CUMPLIR EN EL TRATAMIENTO DE DATOS PERSONALES

Deber de Confidencialidad

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

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

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

Deber de Seguridad

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

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

El Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión) es la materialización de los deberes de seguridad y confidencialidad.

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

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

- Integridad: es la propiedad de salvaguardar la exactitud y completitud de la información, así como evitar la modificación no autorizada o accidental de la misma.

- ❖ Confidencialidad: es la propiedad de la información para no estar a disposición o ser revelada a personas no autorizadas.
- ❖ Disponibilidad: es la propiedad de un dato para ser accesible y utilizable, prevenir interrupciones no autorizadas.

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

a) Crear políticas internas para la gestión y tratamiento de los datos personales.
b) Elaborar un inventario de datos personales.
c) Definir funciones y obligaciones del personal que trate datos personales.
d) Realizar un análisis de riesgo de los datos personales, el cual deberá considerar amenazas, vulnerabilidades existentes y recursos involucrados en el tratamiento.
e) Realizar un análisis de brecha. (consistente en comparar las medidas de seguridad existentes contra las medidas de seguridad faltantes.
f) Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes y el cumplimiento cotidiano de sus políticas de gestión.
g) Monitorear y revisar de manera periódica las medidas de seguridad implementadas.
h) Diseñar y capacitar al personal del responsable.

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

Fase 1. Planear el SGSDP
- ✓ Paso 1. Establecer el Alcance y Objetivos
- ✓ Paso 2. Elaborar una Política de Gestión de Datos Personales
- ✓ Paso 3. Establecer Funciones y Obligaciones
- ✓ Paso 4. Elaborar un Inventario de Datos Personales
- ✓ Paso 5. Realizar un Análisis de Riesgo de Datos Personales
- ✓ Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha

Fase 2. Implementar el SGSDP
- ✓ Paso 7. Implementación de las Medidas de Seguridad aplicables a los Datos Personales

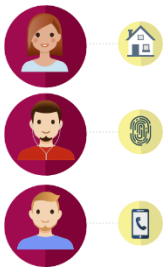
Fase 3. Monitorear y Revisar el SGSDP
- ✓ Paso 8. Revisiones y Auditoria

Fase 4. Mejorar el SGSDP
- ✓ Paso 9. Mejora Continua

La realización e implementación de este Sistema de Gestión de Seguridad de Datos Personales, se podrá tomar como base para la creación del Documento de Seguridad.

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

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



- Riesgo inherente a los datos personales.
- Sensibilidad de los datos personales.
- Desarrollo tecnológico.
- Las posibles consecuencias de una vulneración para los titulares.
- Las transferencias de datos personales que se realicen.
- Numero de titulares.
- Las vulneraciones previas ocurridas en los sistemas de tratamiento.
- El riesgo por el valor cuantitativo y cualitativo respecto de una tercera.
- persona no autorizada.

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

A través de los siguientes mecanismos:

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

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

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

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

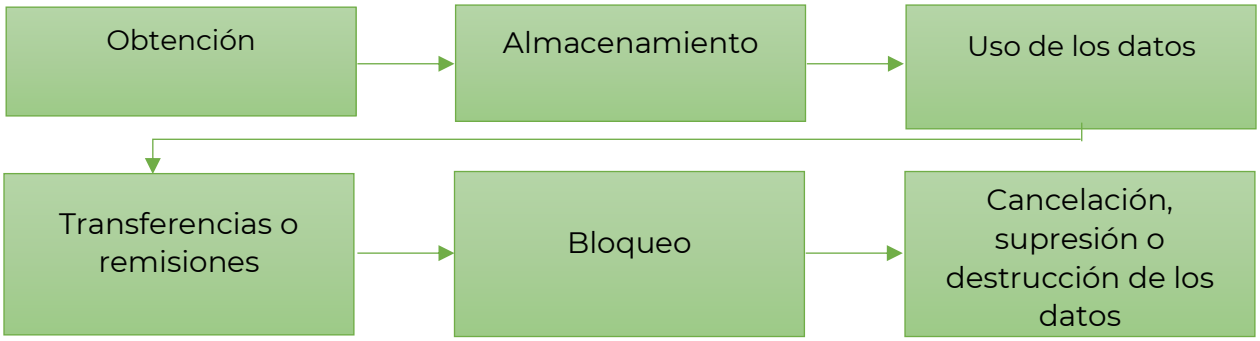
Cabe destacar que las políticas internas para la gestión de los datos personales deben establecer el compromiso de cumplir con la legislación en la materia, por parte de todos los involucrados en el tratamiento a su vez que ésta debe ser comunicada.

El Comité de Transparencia, de CONALEP desarrolló y aprobó las Políticas Internas para la Gestión y el Tratamiento de Datos Personales en posesión del CONALEP.

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

Es necesario elaborar un inventario con la información de cada tratamiento de datos que se realice, que contenga un catálogo de medios físicos y electrónicos, finalidades, tipo de datos tratados, formatos de almacenamiento, lista de los servidores públicos que tienen acceso al tratamiento, en su caso, nombre o razón social del encargado, así como de los destinarios de las transferencias.

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



Realizar el inventario de datos personales, implica llevar a cabo un diagnóstico de los datos personales y sistemas de tratamiento que se encuentran bajo resguardo, identificando los siguientes elementos relevantes:

1. Cada uno de los procesos en los que la unidad administrativa trata datos personales.
2. La unidad administrativa que está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.
3. De acuerdo con el ciclo de vida de los datos personales, se debe identificar:
   I. ¿Cómo se obtienen los datos personales?
   II. ¿Qué tipo de datos personales se tratan? ¿Son sensibles?
   III. ¿Dónde se almacenan los datos personales?
   IV. ¿Para qué finalidades se utilizan los datos personales?
   V. ¿Quién tiene acceso a la base de datos o archivos y a quién se comunican los datos personales al interior de la organización?
   VI. ¿Intervienen encargados en el tratamiento de los datos personales?
   VII. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
   VIII. ¿Se difunden los datos personales?
   IX. ¿Cuál es el plazo de conservación de los datos personales?

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

Para definir las funciones y obligaciones del personal involucrado en el tratamiento de datos

personales, se debe atender lo que establece el artículo 57 de Los Lineamientos Generales, que estipula que se deberán establecer y documentar los roles y responsabilidades para todos aquellos que intervienen en el tratamiento de los datos personales dentro de la institución.

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

d) El análisis de riesgos

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

"Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:

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

Para el cumplimiento del análisis de riesgo, se debe realizar considerando lo establecido en los Lineamientos Generales[4] que establecen lo siguiente:

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

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

- Identificar activos
- Identificar amenazas
- Identificar vulnerabilidades

[4] Artículo 60 de los Lineamientos Generales

El INAI elaboró un evaluador de vulneración, que permite a los revisar los posibles riesgos en los tratamientos que realizan a través de una serie de preguntas cerradas, permite generar múltiples evaluaciones y así apoyar y orientar en el cumplimiento de la normativa en materia de protección de datos personales.

e) El análisis de brecha

Es importante establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos, protegiendo los mismos contra daño, perdida, alteración, destrucción o una utilización no autorizada de los mismos.

La Ley General define las medidas de seguridad como el conjunto de acciones y actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales:

Medidas de seguridad administrativas[5]	Medidas de seguridad físicas[6]	Medidas de seguridad técnicas[7]
Se refieren a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.	Son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Se deben considerar, como mínimo, las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.	Abarcan el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Se deben considerar, como mínimo, las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

[5] Artículo 3, fracción XXI de la Ley General

[6] Artículo 3, fracción XXII de la Ley General

[7] Artículo 3, fracción XXIII de la Ley General

Para el análisis de brecha se debe considerar lo siguiente:

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

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

f) El plan de trabajo

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

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

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

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

Como parte de la evaluación de las políticas implementadas en materia de seguridad y tratamiento de los datos personales, debe monitorearse y revisarse, al respecto los Lineamientos Generales[8] establecen que debe supervisarse lo siguiente:

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

[8] Artículo 63 de los Lineamientos Generales

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

a) La pérdida o destrucción no autorizada.
b) El robo, extravío o copia no autorizada.
c) El uso, acceso o tratamiento no autorizado.
d) El daño, la alteración o modificación no autorizada.

Cuando se sufra alguna vulneración a la seguridad, se deberá actuar conforme a lo dispuesto en los artículos 37, 38, 39, 40 y 41 de la Ley General y, para el caso de las notificaciones sobre vulneraciones, deberá observar los artículos 66, 67 y 68 de los Lineamientos Generales.

h) El programa general de capacitación

Diseñar e implementar programas a corto, mediano y largo plazo, para los involucrados en el tratamiento de los datos personales, atendiendo a sus roles, funciones y responsabilidades asignados, a fin de contar con personal consciente de sus responsabilidades y deberes respecto de la protección de datos personales, para lo cual, se deben establecer y mantener programas de capacitación considerando las siguientes etapas:

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

DOCUMENTO DE SEGURIDAD

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

Este documento de manera particular deberá contener lo siguiente:

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

El contenido del documento de seguridad se integra por una serie de acciones que se deben realizar para garantizar la seguridad de los datos personales, mismas que ya se señalaron en el presente documento.

La seguridad de los datos personales debe observarse durante todo su ciclo de vida, desde su obtención hasta su eliminación.

El documento deberá actualizarse cuando ocurran los siguientes eventos:

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

¿Qué hacer en caso de una vulneración de seguridad?

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

¿A quién debo informar en caso de una vulneración?

Se deberá notificar al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y a los titulares.

Al órgano garante deberá informar lo siguiente:

- Hora y fecha de la vulneración.
- Hora y Fecha del inicio de la investigación.
- Naturaleza de la vulneración ocurrida.

- La descripción de las circunstancias en torno a la vulneración.
- Las categorías y número aproximado de titulares afectados.
- Los sistemas de tratamiento y datos personales comprometidos.
- Las acciones correctivas realizadas.
- La descripción de las posibles consecuencias de la vulneración.
- Las recomendaciones dirigidas al titular.
- El medio puesto a disposición del titular para que pueda obtener más información al respecto.
- El nombre completo de las personas designadas que puedan proporcionar más información al Instituto;
- Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

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

- La naturaleza de la vulneración.
- Los datos personales comprometidos.
- Las recomendaciones para que los titulares puedan proteger sus intereses.
- Las acciones correctivas realizadas.
- Los medios para que el titular pueda obtener más información.
- La descripción de las circunstancias generales en torno a la vulneración ocurrida.
- Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

¿Cómo verificar el cumplimiento respecto al Sistema de Gestión?

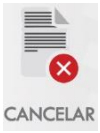
Para conocer una lista de comprobación del contenido de los elementos que debe contener el Sistema de Gestión, dicho listado contempla: el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; los mecanismos de monitoreo y revisión de las medidas de seguridad, y el programa general de capacitación.

EL EJERCICIO DE LOS DERECHOS ARCO

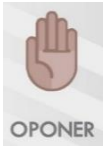
El acrónico ARCO está conformado por las iniciales de los derechos de Acceso, Rectificación, Cancelación y Oposición de los datos personales, que los titulares pueden ejercer y que consisten en:

Derecho de Acceso: Es el derecho que tiene el titular de solicitar el acceso a sus datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes.
Ejemplo: solicitar a una autoridad tributaria, acceso a sus datos de contacto que tenga registrados.

Derecho de Rectificación: Es el derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados.
Ejemplo: cuando un titular solicita un servicio a una Institución, el servidor público que atendió y registró, por error, un domicilio que no corresponde con el del titular, ante esa inexactitud, los titulares tienen el derecho de solicitar la rectificación respectiva, acreditando el domicilio correcto.



Derecho de Cancelación: Es el derecho que tienen los titulares de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas y/o bases de datos. Hay que tomar en cuenta que no en todos los casos se podrán eliminar sus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.
Ejemplo: En un otorgamiento de becas por un año, está ya concluyó, la institución sigue enviando trimestralmente un correo electrónico con una encuesta relacionada con la beca otorgada. A través del ejercicio del derecho de cancelación, el titular puede solicitar a la institución que borre su información de los registros, con la finalidad de ya no recibir dichos correos, pues ya concluyó la finalidad para la cual obtuvieron y trataron sus datos.

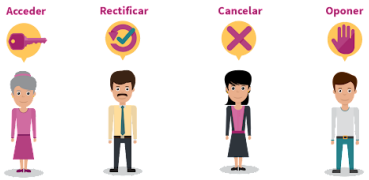


Derecho de Oposición Es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para una determinada finalidad, no para la totalidad de estas. No siempre se podrá impedir el uso de los datos, cuando estos sean necesarios por motivos legales o para el cumplimiento de obligaciones.
Ejemplo: Cuando un asistente a un curso en una Institución Gubernamental que imparte capacitación recaba un correo electrónico el cual utiliza para enviar invitaciones a eventos y también para enviar un boletín informativo, el titular puede oponerse a una finalidad específica, pero desear recibir aún invitaciones para eventos futuros. A partir del ejercicio del derecho de oposición, el titular puede solicitar al responsable que no envié el boletín.

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

Las causas por las que el responsable puede negar el ejercicio de los derechos ARCO[9] son:

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



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

¿Cómo se ejercen los derechos ARCO?

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

Para que un derecho sea ejercido no es necesario que se haya ejercido previamente otro, ni el ejercicio de uno impide que posteriormente se ejerza uno distinto.

Por ejemplo, un titular puede solicitar a una dependencia en su carácter de responsable la rectificación de sus datos personales sin que previamente haya ejercido su derecho de acceso.

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

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

Los requisitos que debe tener la solicitud son:

a) El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones.
b) Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.
c) De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud.
d) La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso.

[9] Artículo 55 de la Ley General

e) La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular.
f) Cualquier otro elemento o documento que facilite la localización de los datos personales.

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

- Derecho de ACCESO: la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
- Derecho de RECTIFICACIÓN: las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
- Derecho de CANCELACIÓN: las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
- Derecho de OPOSICIÓN: las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

Si la solicitud no cuenta con la información antes descrita, el responsable podrá solicitar la información faltante por medio de una PREVENCIÓN, la cual se deberá emitir en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, y tendrán 10 días hábiles, después de recibir la prevención, para proporcionar la información requerida, pues de lo contrario se tendrá como no presentada su solicitud.

Previo a que se ejerza el derecho de acceso, rectificación, cancelación u oposición se deberá acreditar la identidad del titular de los datos personales y, en su caso, de su representante.

Hay tres medios para acreditar la identidad:

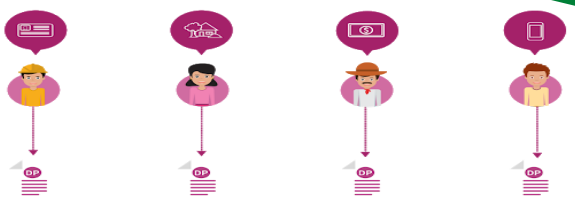
- Identificación oficial con fotografía.
- Instrumentos electrónicos o mecanismos de autenticación, como la Firma Electrónica.
- Mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

Por su parte el representante deberá acreditar su personalidad mediante:

- Copia de identificación oficial con fotografía del titular de los datos;
- Identificación del representante;
- Instrumento notarial o Carta Poder (firmada por dos testigos y sus respectivas identificaciones)

En el caso de las solicitudes de ejercicio de derechos ARCO de una persona menor de edad, en estado de interdicción o incapacidad legal, cuando se pretenda ejercer los derechos ARCO se deberá de observar lo dispuesto en las leyes civiles y la representación será conforme a las reglas que establezca dicha normatividad.

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



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

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

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

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

- Acta de nacimiento del menor de edad;
- Documento legal que acredite el ejercicio de la patria potestad;
- Documento de identificación oficial de quien ejerce la patria potestad y presenta la solicitud;
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de esta.

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

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

Personas en estado de interdicción o incapacidad legal:

- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de la misma.

Personas fallecidas:

- Identificación oficial de la persona a quien pertenecían los datos personales.
- Acta de defunción correspondiente.
- Documento(s) que acrediten el interés jurídico de quien presenta la solicitud; aquél donde el titular de los datos personales hubiere expresado fehacientemente su voluntad de que esta persona ejerza los derechos ARCO con relación a sus datos personales, o el mandato judicial que en su caso exista para dicho efecto.
- Documento de identificación oficial de quien presenta la solicitud.

Procedimiento y plazos en una solicitud de ejercicio de derechos ARCO

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

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

Paso 1. Recepción de la solitud formulada por el titular o su representante. La solicitud debe acusarse de recibida constando fecha de esta.

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

Paso 3. En caso de que haya procedido el ejercicio del derecho, el responsable llevará a cabo las acciones necesarias para hacerlo efectivo (15 días hábiles).

Ahora bien, si la solicitud no cuenta con la información suficiente en su solicitud para el ejercicio de los derechos ARCO, entre el paso 1 y 2, se podrá solicitar al titular que proporcione la información faltante por medio de un escrito denominado prevención.

Cuando la normatividad aplicable a determinados tratamientos de datos personales establezca un trámite o procedimiento diferente para solicitar el ejercicio de derechos ARCO, se deberá informar al titular sobre la existencia de dicho trámite o procedimiento en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, a fin de que el titular decida si presentará su solicitud de ejercicio de derechos ARCO de acuerdo con el trámite específico o con base en el procedimiento establecido en la Ley General.

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

La información deberá ser entregada sin costo cuando implique la entrega de no más de veinte hojas simples[10]

Las obligaciones vinculadas a los derechos ARCO
Obligaciones generales:

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

La relación entre el responsable y el encargado y las obligaciones que cumplir

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

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

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

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. Los acuerdos que se alcancen entre el responsable y el encargado deberán ser acordes con lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales y no deberá contravenir lo estipulado en la Ley General.

[10] Párrafo tercero del artículo 50 de la Ley General

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

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

I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
V. Guardar confidencialidad respecto de los datos personales tratados;
VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales,
VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente

De acuerdo con el numeral 61 de la Ley General, el encargado puede llevar a cabo subcontrataciones, siempre que cuente con la autorización del responsable, es decir, que se establezca en el instrumento jurídico.

Una vez obtenida la autorización, 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.

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

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

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

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

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

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

De igual manera deberá contar con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos;
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.

Obligaciones ligadas a la relación entre el responsable y el encargado:
El responsable tiene las siguientes obligaciones respecto de la relación que establezca con los encargados que traten datos a nombre del responsable, deberán contar con lo siguiente:

1. La relación con los encargados debe formalizarse mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido.
2. Incluir en el contrato o instrumento jurídico, al menos las siguientes cláusulas con encargado:

- El tratamiento de datos personales deber realizarse conforme a las instrucciones del responsable;

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

3. Informar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones antes señaladas.

Las transferencias y las obligaciones que cumplir

Transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta del titular, del responsable o del encargado.

Ejemplo: Cuando el responsable comunica los datos del servidor público al ISSSTE, a fin de que se otorguen las prestaciones que le corresponden por ley.

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

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

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

- Cuando una ley así lo disponga;
- Cuando las transferencias que se realicen entre responsables, para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento;
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- Para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica;
- Cuando exista una situación de emergencia;
- Asistencia sanitaria;
- Los datos se encuentren en fuentes de acceso público;
- Los datos personales sean sometidos a un procedimiento de disociación;
- El titular de los datos sea una persona reportada como desaparecida;
- Transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal;
- Transferencia sea internacional, en cumplimiento en una ley o tratado internacional suscrito y ratificado por el estado mexicano;
- A petición de una autoridad u organismo extranjero, competente en su carácter de receptor, cuyas facultades sean homologas;
- Transferencia necesaria por un contrato celebrado o por celebrar en interés del titular;
- La transferencia sea necesaria por razones de seguridad.

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

Requisitos para transferencia nacionales

Condición específica	Receptor de los datos	Formalización
1. Ser informada en el aviso de privacidad 2. Solicitar el consentimiento del titular cuando se requiera 3. Limitarse a las transferencias consentidas e informadas.	El receptor de los datos personales adquirirá el carácter de responsable con las obligaciones respectivas y deberá tratar los datos conforme a lo convenido en el aviso de privacidad que le comunique el transferente.	Deberá formalizarse mediante algún mecanismo que permita demostrar que el transferente comunicó al receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.

Requisitos para transferencias internacionales

Condición específica	Receptor de los datos	Formalización
1. Serán posibles cuando el receptor de los datos asuma las mismas obligaciones a las que se encuentra el responsable que transfiere los datos personales. 2. Ser informada en el aviso de privacidad 3. Solicitar el consentimiento del titular cuando se requiera. 4. Limitarse a las finalidades consentidas e informadas.	El receptor de los datos personales NO podrá considerarse un responsable en términos de la Ley General, pues al no estar establecido en territorio nacional, no le aplica la norma mexicana. Mediante el instrumento jurídico en el que se establezca la relación con el transferente, los datos personales, deberá asumir las mismas obligaciones que éste tiene con relación al tratamiento de los datos personales. Si el receptor de los datos no acepta estas condiciones, a quien sí le aplica la ley mexicana, NO podrá transferirle los datos personales.	El transferente puede valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones para el receptor, a las que se encuentra sujeto, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

En caso de dudas en las transferencias internacionales se podrá solicitar opinión del INAI, cumpliendo los requisitos establecidos en el artículo 117 de los Lineamientos Generales.

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

Obligaciones ligadas a las transferencias:

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

1. Todas las transferencias deben formalizarse mediante la suscripción de un instrumento jurídico, que establezca el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades contraídas por las partes, salvo en las siguientes excepciones:

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

- Cuando sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o derivado de una petición de la autoridad extranjera u organismo internacional en su carácter de receptor, cuando las facultades entre el sujeto obligado y el responsable receptor sean homólogas, o también, cuando las finalidades de la transferencia sean análogas respecto de aquéllas que dieron origen al tratamiento.

2. Sólo hacer transferencias fuera del territorio nacional cuando el tercero receptor se obligue a proteger los datos personales conforme a los principios y deberes que establece la Ley General y demás disposiciones aplicables en la materia.
3. Comunicar el aviso de privacidad respectivo al tercero receptor en las transferencias nacionales e internacionales que se realicen.
4. Solicitar el consentimiento para las transferencias nacionales e internacionales, salvo en los siguientes casos:

   - Cuando sea nacional y se realice entre el sujeto obligado y otros responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.
   - Cuando se encuentre prevista en una ley o tratado suscrito y ratificado por México.
   - Cuando sea entre responsables y derivado de sus atribuciones análogas o compatibles con la finalidad que dio origen al tratamiento.
   - Cuando se trate una transferencia legalmente exigida para la investigación y persecución de los delitos, o bien, la procuración o administración de justicia.
   - Cuando precisa para el reconocimiento, ejercicio o defensa de un derecho.
   - Cuando tenga como finalidad el mantenimiento o cumplimiento de una relación jurídica entre el sujeto obligado y el titular.
   - Cuando sea necesaria por virtud de un contrato en interés del titular, por el sujeto obligado y un tercero.
   - Cuando se trate de los casos establecidos en el artículo 22 de la Ley General.
   - Sea necesaria por razones de seguridad nacional.

5. Establecer el medio para obtener el consentimiento expreso del titular de forma previa a la transferencia de los datos personales.
6. En caso de que la transferencia sea nacional, el receptor deber observar la confidencialidad y la obligación de utilizar los datos personales únicamente para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad.

¿Cómo cumplo con las obligaciones derivadas de las transferencias?

Actividades para su cumplimiento

1) Identificar las transferencias que se realizan que requieren la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.
2) Elaborar y suscribir las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, cuando se requiera.
3) Para las transferencias y remisiones internacionales, previo a que éstas ocurran, se deberá solicitar al tercero receptor que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la Ley General.
4) Cuando inicien las transferencias, comunicar el aviso de privacidad correspondiente.
5) Identificar las transferencias que requieren consentimiento de los titulares e informarlo en el aviso de privacidad.
6) Solicitar el consentimiento de los titulares previo a la transferencia según la modalidad que se requiera.
7) Establecer los medios para solicitar el consentimiento expreso, previo a la transferencia.
8) Implementar los controles de seguridad establecidos para la confidencialidad de los datos personales, y no tratar los datos personales para finalidades distintas.

Sanciones

El incumplimiento de las obligaciones en el tratamiento de Datos Personales implica vulnerar el derecho humano a la protección de datos personales, por lo que, puede dar lugar a la imposición de medidas de apremio y sanciones

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), puede imponer como medidas de apremio, la amonestación pública o una multa equivalente a la cantidad, de ciento cincuenta hasta mil quinientas veces del valor de la unidad de medida y las multas no podrán ser cubiertas con recursos públicos.

El incumplimiento será difundido en los portales de obligaciones de transparencia del INAI y serán considerados en la evaluación que éste realice.

Mediante un procedimiento de verificación, el INAI ejerce sus facultades para la vigilancia y verificación del cumplimiento de las disposiciones de la Ley General, este procedimiento puede iniciar de oficio cuando el INAI presuma de manera fundada y motivada la existencia de incumplimiento a la Ley General, también puede iniciar por denuncia de los titulares, este procedimiento concluye con una resolución del INAI, en la que se establecerán las medidas que correspondan.

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

- Actuar con negligencia, dolo o mala fe, dolo en el procedimiento para el ejercicio de los derechos ARCO.

- Por incumplimiento en los plazos para atención a las solicitudes para el ejercicio de los derechos ARCO.
- Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente los datos personales que se tengan en custodia.
- En forma intencional, tratar los datos personales violando los principios y deberes.
- No contar con el aviso de privacidad, o que este no cuente con todos los elementos informativos.
- Clasificar como confidencial, con dolo o negligencia.
- Incumplir el deber de confidencialidad.
- No establecer las correctas medidas de seguridad.
- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.
- No observar lo dispuesto en la normatividad en el caso de las transferencias.
- Obstruir los actos de verificación de la autoridad.
- Crear bases de datos personales en contravención a los dispuesto, para considerarse fuente de acceso público.
- No acatar las resoluciones emitidas por el INAI.

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

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

Referencias

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Publicada en el DOF. el 26 de enero de 2017.

Lineamientos Generales de Protección de Datos Personales para el Sector Público ACT-PUB/19/12/2017.10

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

Procedimiento para ejercer los Derechos ARCO para el sector público

Cuadernillo “Uso de Datos Personales”. Policía Federal