BASE DE DATOS DE LEGISLACIÓN Y JURISPRUDENCIA

I.N.A.I. (INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES)

Normativa y legislación en PDP

Leyes en México para la protección de datos personales

Fundamento constitucional y nociones generales

La protección de datos personales es un derecho humano, reconocido en el artículo 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, el cual establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición.[1]

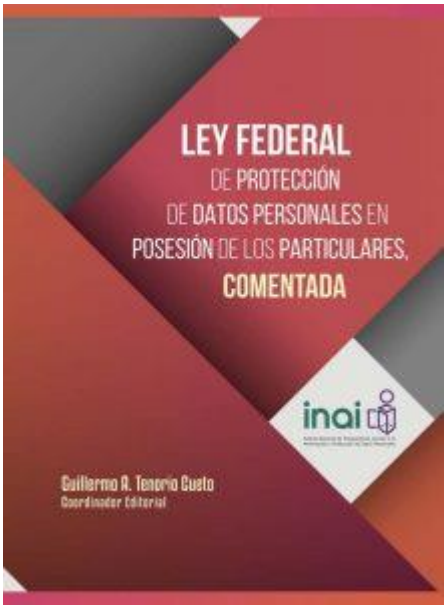
En México, el derecho a la protección de datos personales se encuentra regulado en diversos ordenamientos según el ámbito de que se trate. Por lo que se refiere al ámbito privado tenemos la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), mientras que en el sector público existe la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). Con la entrada en vigor de esta última normativa, las leyes de ambos sectores – público y privado- establecieron una serie de principios con las reglas y obligaciones que rigen el tratamiento de datos personales por parte del responsable.

Adicionalmente, cada entidad federativa de México debe contar con una Ley que regule el tratamiento de datos personales en el sector público, según su ámbito territorial, y que esté armonizada con la LGPDPPSO.

Por tratamiento de datos personales se entiende cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento,

posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales.[2]

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.



Objeto

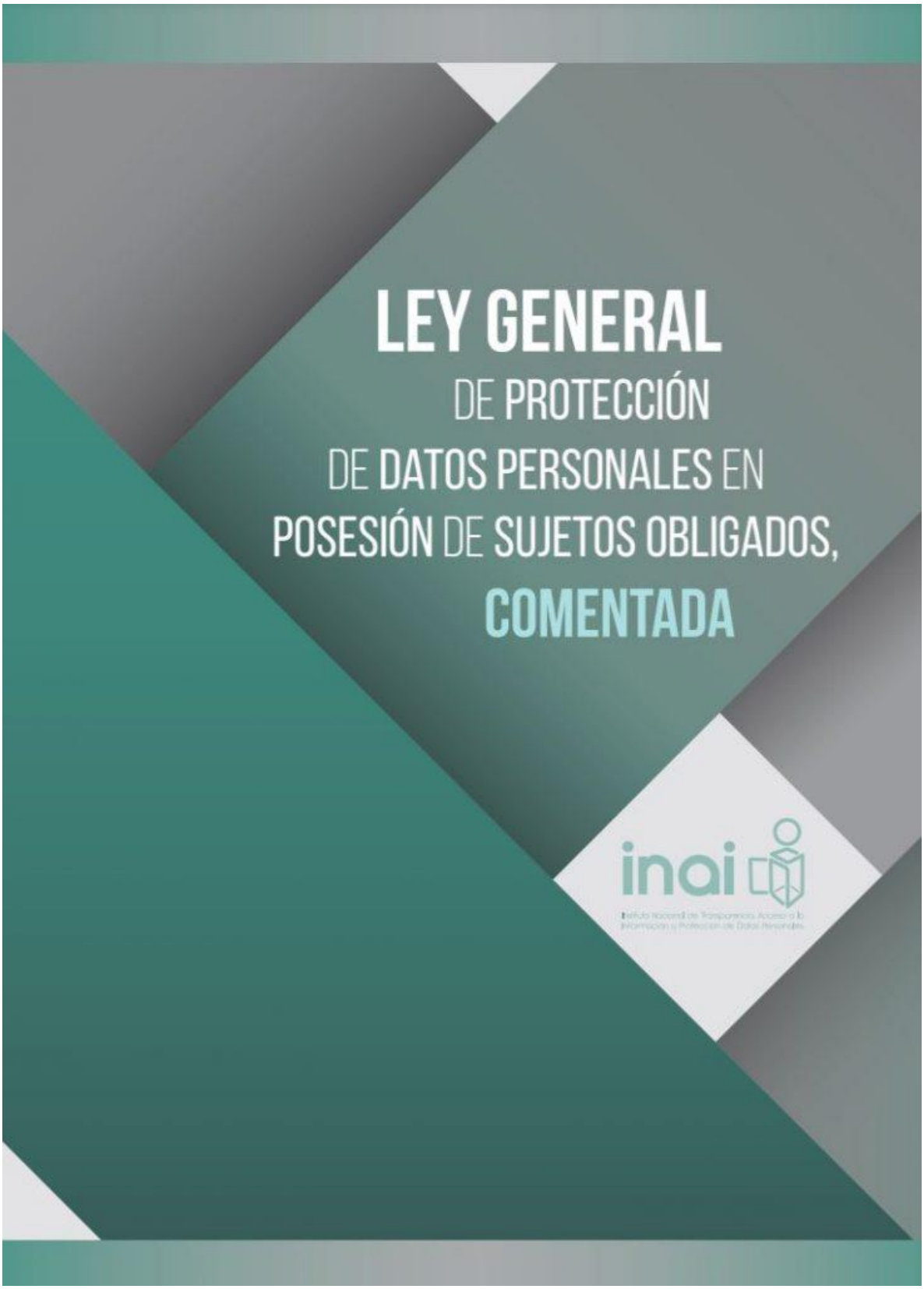
La LFPDPPP, publicada en el Diario Oficial de la Federación el 5 de julio de 2010, tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su **tratamiento**[1] legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la **autodeterminación informativa**[2] de las personas.

[1] El tratamiento de datos personales implica la obtención, uso, divulgación o almacenamiento de datos personales. El uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia, comunicación o disposición de datos personales.

[2] La autodeterminación informativa implica el derecho de las personas para decidir, de manera libre e informada, sobre el uso de la información que les pertenece.

¿A quién aplica?

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados


LEY GENERAL
DE PROTECCIÓN
DE DATOS PERSONALES EN
POSESIÓN DE SUJETOS OBLIGADOS,
COMENTADA
inai

Objeto

La LGPDPPSO, publicada en el Diario Oficial de la Federación el 26 de enero de 2017, tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados.

¿A quién aplica?

Principios y derechos de protección de datos personales

Tanto la LFPDPPP como la LGPDPPSO contemplan que los responsables del tratamiento de datos personales deberán observar los siguientes principios:

1. Licitud
2. Consentimiento
3. Información
4. Calidad
5. Finalidad
6. Lealtad
7. Proporcionalidad
8. Responsabilidad

Dichos principios se traducen en obligaciones concretas para los responsables del tratamiento.

A continuación, se describirá el contenido de cada uno de los principios, así como de las obligaciones ligadas a estos[1].

Licitud

El principio de licitud implica que los responsables deben tratar los datos personales de manera lícita, conforme a lo dispuesto por la legislación mexicana y el derecho internacional aplicable, así como por la normativa que le resulte aplicable a cada responsable.

Obligaciones ligadas al principio de licitud. El principio de licitud establece que ni los responsables ni nadie puede tratar los datos personales para actividades ilícitas, ni de forma tal que contravenga lo dispuesto por la LFPDPPP, la LGPDPPSO, ni en ningún otro ordenamiento vigente en México, o acuerdo internacional del cual el país sea parte.

Por ejemplo, si se descarga una aplicación para recibir noticias personalizadas semanalmente, y la empresa vende los datos personales a un partido político para que manden publicidad durante la campaña electoral, la empresa responsable estaría violando el principio de licitud, pues en este caso no se otorgaron los datos personales para esa finalidad, sino únicamente para recibir los servicios de noticias semanalmente; por lo tanto, también el partido político estaría violando las disposiciones de la Ley que le es aplicable al tratar datos personales sin consentimiento.

Consentimiento

Este principio consiste en que, como regla general[1], el responsable debe obtener el consentimiento de la persona a quien pertenecen los datos personales, antes de utilizarlos. La solicitud de consentimiento debe ir siempre ligada a las finalidades concretas del tratamiento, las cuales se encuentran previstas en el aviso de privacidad correspondiente.

El consentimiento del titular puede manifestarse de forma expresa o tácita. El consentimiento es **tácito** cuando, habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por ejemplo, si después de haber recibido la información el titular no dice que no, se considera que su consentimiento es tácito.

Por su parte, el consentimiento es **expreso** cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología. Por ejemplo, antes de descargar un juego en línea, te piden marcar una casilla para indicar que estás de acuerdo con la política de privacidad y las condiciones de uso de dicho juego.

Salvo que alguna Ley exija el consentimiento expreso del titular, se considera que es válido el consentimiento tácito para todo tratamiento de datos personales.

Asimismo, para que el consentimiento tácito o expreso[2] sea válido, se requiere que sea:

- **Libre:** sin que medie error, mala fe (se busca obtener un beneficio sin el afán de causar daño a una persona), violencia o dolo (se tiene la voluntad de cometer un delito a sabiendas de que es ilícito) que puedan afectar la manifestación de voluntad del titular.
- **Específico:** que se refiera a finalidades determinadas y concretas que justifiquen el tratamiento.
- **Informado:** que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos.
- **Inequívoco:** el consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.

Obligaciones ligadas al principio de consentimiento. El principio de consentimiento implica, entre otras, las siguientes obligaciones para los responsables:

1. Los responsables deben obtener el consentimiento para el tratamiento de tus datos personales, salvo que se actualice alguno de los supuestos de excepción previstos en la normativa aplicable.
2. El consentimiento siempre debe ir ligado a finalidades específicas e informadas en el aviso de privacidad.
3. En caso de que los datos personales a tratar sean sensibles, el responsable deberá solicitar un consentimiento expreso y por escrito.

Recordemos que los datos personales sensibles son aquellos datos tales como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y

morales, afiliación sindical, opiniones políticas, preferencia sexual; que afectan la esfera más íntima de la persona, o cuyo mal uso pueda ser causa de discriminación o provocarle un riesgo grave.

Un ejemplo de violación al principio de consentimiento ocurre cuando el titular acude a realizarse estudios médicos con un especialista y éste recaba algunos datos personales sensibles como el tipo de sangre, historial clínico, entre otros, pero no obtiene el consentimiento expreso y por escrito para el tratamiento de dichos datos sensibles.

[1] Las leyes contemplas excepciones en donde el responsable no está obligado a recabar los datos personales del titular.

Información

El principio de información obliga a los responsables a informar a los titulares, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, con una estructura y diseño que facilite su entendimiento, con la finalidad de que sea un mecanismo de información práctico y eficiente. La información que, en general, se debe hacer del conocimiento de los titulares a través del aviso de privacidad es la siguiente:

- La **identidad y domicilio** del responsable que trata los datos personales.
- Los **datos personales que serán sometidos a tratamiento**, identificando aquellos que son sensibles.
- Las **finalidades** del tratamiento.
- Los **mecanismos para que el titular pueda manifestar su negativa** al tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable.
- Las **transferencias**[1] de datos personales que, en su caso, se efectúen, así como la cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera. Las transferencia de datos personales: Se refiere a la comunicación de datos que realiza el responsable del tratamiento a un tercero, distinto del titular, del mismo responsable o del encargado.
- Los medios y el procedimiento para **ejercer los derechos ARCO**.
- Las opciones y medios que el responsable ofrece al titular para **limitar el uso o divulgación** de los datos personales[2].
- La información sobre el **uso de mecanismos en medios remotos** o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos. Es decir, si usan herramientas como cookies, a través de las cuales es posible obtener datos

personales sobre tus hábitos, tus preferencias, tu ubicación o sobre tu navegación en general en internet.

- Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los **cambios al aviso de privacidad**.

Esta información puede variar dependiendo de la modalidad del aviso de privacidad (corto, simplificado o integral) y si la institución del responsable es pública o privada.

El aviso de privacidad integral siempre deberá estar a disposición para su consulta por parte de los titulares, por ello tanto en el aviso de privacidad corto como en el simplificado, te deben informar dónde puedes consultar el integral, que es la versión que contiene toda la información que señala la Ley. La diferencia entre estas tres modalidades consiste en la información que contienen.

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

1. Deberá poner a disposición el aviso de privacidad, aunque no se requiera el consentimiento de para el tratamiento de los datos personales.
2. El responsable deberá poner a disposición el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera directa o personal del titular.
3. El aviso de privacidad debe estar redactado de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento. No deberá usar frases inexactas, ambiguas o vagas; deberá tomar en cuenta los perfiles de los titulares; no tiene que 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.
4. El aviso de privacidad tiene que estar ubicado en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.

Para reforzar el principio de información, así como los elementos que debe contener el aviso de privacidad, se sugiere desarrollar la *Actividad 5*.

Calidad

El principio de calidad radica en que los datos personales tratados deben ser exactos, completos, pertinentes, actualizados y correctos según se requiera para el cumplimiento de la finalidad para la cual son tratados.

Los datos personales son **exactos** cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. Por ejemplo, un dato no sería exacto si se registra en la base de datos un error en el nombre o apellidos del titular de la cuenta (si el nombre del titular es “Juan Pérez González” y en la base de datos aparece “Juan González Pérez” dichos datos no serían exactos).

Los datos personales están **completos** cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados de forma tal que no se cause un daño o perjuicio al titular. Por ejemplo, los datos de salud del titular están completos cuando el

expediente médico que obra en el hospital contiene todos los documentos clínicos e información que debe estar integrada al mismo.

Los datos personales son **pertinentes** cuando corresponden efectivamente al titular. Por ejemplo, los datos de un adeudo son pertinentes cuando corresponden al deudor.

Los datos están **actualizados** cuando están al día y corresponden a la situación real del titular. Por ejemplo, un dato no se encuentra actualizado cuando en tu identificación oficial (INE) aparece un domicilio antiguo que no corresponde al que resides en la actualidad.

Los datos personales son **correctos** cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

Este principio también implica que 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: i) las disposiciones legales aplicables en la materia de que se trate; ii) los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y iii) el periodo de bloqueo[1].

En este sentido, el plazo de conservación es igual al tiempo requerido para llevar a cabo las finalidades del tratamiento, más los plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables, y el periodo de bloqueo.

Tiempo requerido para llevar a cabo las finalidades del tratamiento

\+ Plazos legales, administrativos, contables, fiscales, jurídicos e históricos

\+ Período de bloqueo

= PLAZO DE CONSERVACIÓN

Obligaciones ligadas al principio de calidad. Las principales obligaciones relacionadas con el principio de calidad son las siguientes:

1. Adoptar medidas para que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia una afectación para el titular.
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, así como el periodo de bloqueo.

3. Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo solo 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.

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

Finalidad

De conformidad con el principio de finalidad, los datos personales únicamente podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad. La finalidad o las finalidades establecidas en el aviso de privacidad deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva, se especifica para qué objeto serán tratados los datos personales.

Algunas finalidades son necesarias para la relación que se pretende establecer con el responsable del tratamiento de los datos personales; por ejemplo, cuando se acude a un centro médico para una revisión, es necesario que el doctor obtenga y trate los datos personales para dar atención médica, o bien, cuando se realiza una compra en internet en una tienda virtual, es necesario que recaben y utilicen los datos personales para poder ofrecer el servicio o vender el producto.

En estos casos, si el médico o la tienda virtual no obtienen y utilizan esos datos personales, resultará imposible que puedan brindar el tratamiento médico o entregar el producto que se desea obtener. Por ello, a estas finalidades se les llama primarias o principales.

En cambio, hay otras finalidades que no son necesarias para la relación con el responsable, por ejemplo, cuando los datos personales que se proporcionaron para la atención médica o para la compra del producto se utilizan para que el centro médico o la tienda virtual envíen publicidad.

Estas finalidades se conocen como secundarias y no son indispensables que ocurran, por lo que, en general, para ellas el responsable debe requerir el consentimiento, mismo que se puede retirar en cualquier momento.

Obligaciones ligadas al principio de finalidad. El principio de finalidad implica 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. Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales.

Para reforzar el principio de finalidad, se sugiere desarrollar la *Actividad 6*.

Lealtad

El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

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

- No se recaben datos personales con dolo, mala fe o negligencia.
- No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado.
- Se informen todas las finalidades del tratamiento en el aviso de privacidad.

Obligaciones ligadas al principio de lealtad. El principio de lealtad obliga a los responsables a no hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales, y respetar en todo momento la expectativa razonable de privacidad del titular, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes.

Proporcionalidad

El principio de proporcionalidad obliga al responsable a tratar únicamente los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. Asimismo, el responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.

Obligaciones ligadas al principio de proporcionalidad. Las principales obligaciones respecto al principio de proporcionalidad son las siguientes:

1. Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.
2. Tratar el menor número posible de datos personales, según las finalidades que motivan su tratamiento.
3. Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.

Por ejemplo, si se desea suscribir a una revista digital de deportes y para realizar la suscripción se pide información relacionada con el tipo de sangre del titular, se estaría violando el principio de proporcionalidad, pues en este caso es innecesario que la revista conozca dicha información para brindar el servicio relativo a la suscripción.

Responsabilidad

El principio de responsabilidad consiste en la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y

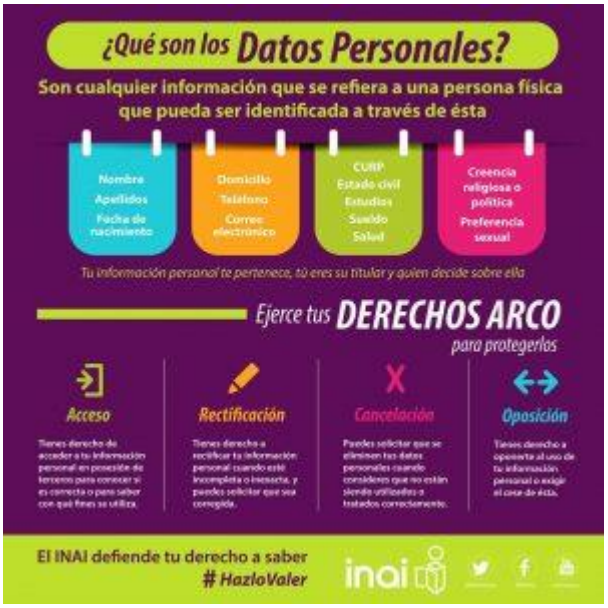
demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

Obligaciones ligadas al principio de responsabilidad. Conforme al principio de responsabilidad, los responsables deberán velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, así como adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.

Para reforzar la aplicación de todos los principios referidos con anterioridad, se sugiere desarrollar la *Actividad 7*.

Derechos

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, reconoce el derecho que tienen los ciudadanos para acceder, rectificar y cancelar sus datos personales, así como oponerse a su uso. A estos derechos se les conoce como derechos ARCO, y se encuentran reconocidos tanto en la LFPDPPP como en la LGPDPPSO.



Derecho de Acceso

Derecho de Rectificación

Derecho de Cancelación

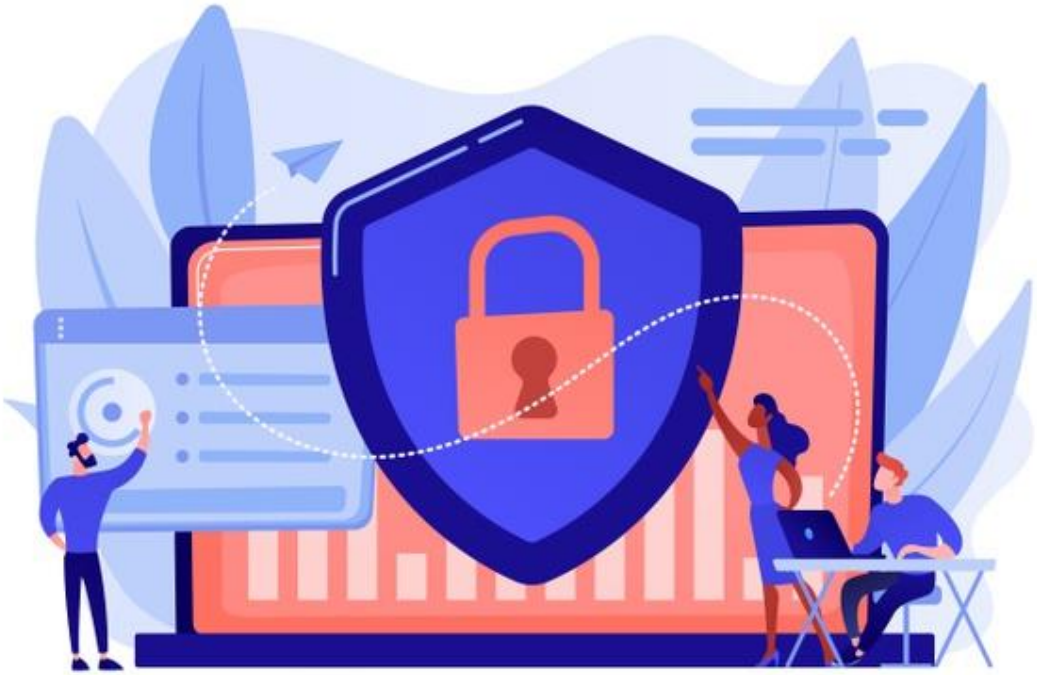
Derecho de Oposición

Es el derecho que tienen los titulares a acceder a sus datos personales que obren en posesión del responsable, ya sea en bases de datos, archivos, registros, expedientes o sistemas, así como a conocer la información relacionada con las condiciones y generalidades del tratamiento.

Por ejemplo, por medio de tu derecho de acceso a datos personales, podrías solicitar a la Secretaría de Educación Pública tu certificado de primaria o secundaria, o bien, algún otro dato personal que se encuentre en posesión de tal dependencia.

Deberes

Además de los principios y obligaciones referidas con anterioridad, los responsables del sector público y privado deben de cumplir con los deberes de seguridad y confidencialidad, mismos que serán desarrollados a continuación.



Deber de seguridad

El deber de seguridad refiere a la obligación de establecer y mantener medidas de seguridad administrativas, físicas y técnicas con el propósito de proteger los datos personales contra daño, perdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.[1]

Las medidas de seguridad administrativas son controles que ayudan a evitar prácticas inadecuadas del personal que pongan en riesgo los datos personales; por ejemplo, dicha medida puede consistir en capacitación al personal que trata datos personales, con el objeto de evitar cualquier vulneración a los mismos.

Por su parte, las medidas físicas son controles aplicados en los espacios físicos e infraestructura que minimicen el robo o acceso no autorizado; por ejemplo, mantener las áreas de trabajo, mobiliario y equipos debidamente cerrados con los controles y candados suficientes.

Finalmente, las medidas técnicas consisten en controles para proteger los equipos de cómputo y dispositivos de almacenamiento de cualquier virus o *malware*; por ejemplo, dichas medidas pueden consistir en la instalación de antivirus en los dispositivos tecnológicos o en la implementación de una política de respaldos de la información.

Deber de confidencialidad

El deber de confidencialidad implica que el responsable debe guardar secreto respecto de los datos personales que son tratados, es decir, que los datos personales del titular no se difundan o compartan con terceros, salvo que se cuente con el consentimiento para ello, o bien, por alguna obligación normativa que exija su difusión.

Para garantizar el cumplimiento del deber de confidencialidad, los responsables tienen que establecer medidas durante todas las fases del tratamiento de los datos personales, incluso después de finalizar la relación con el titular.

Por ejemplo, cuando se proporcionan datos personales en alguna plataforma digital de música o entretenimiento, como podría ser nombre o número de tarjeta, estas empresas deben de establecer medidas para guardar la confidencialidad de dichos datos, ya que, de revelarse tal información, se podría ocasionar un daño patrimonial al titular de la tarjeta y la empresa responsable podría ser sancionada.