



SISTEMA NACIONAL  
DE TRANSPARENCIA  
ACCESO A LA INFORMACIÓN PÚBLICA  
Y PROTECCIÓN DE DATOS PERSONALES



COMISIÓN  
DE PROTECCIÓN  
DE DATOS PERSONALES



DE LA PROTECCIÓN DE DATOS PERSONALES

# ABC DE LA PROTECCIÓN DE DATOS PERSONALES

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

Comisión de Protección de Datos Personales

México, 2022



# DIRECTORIO

## Personas Comisionadas del INAI

- Blanca Lilia Ibarra Cadena ·
- Josefina Román Vergara ·
- Norma Julieta del Río Venegas ·
- Francisco Javier Acuña Llamas ·
- Adrián Alcalá Méndez ·

## Comisión de Protección de Datos Personales

- Arístides Rodrigo Guerrero García ·  
Coordinador de la Comisión  
Ciudad de México
- José Roberto Agundis Yerena ·  
Secretario de la Comisión  
Quintana Roo

## Mención Especial

- Cinthya Denise Gómez Castañeda ·  
Secretaría de la Comisión de Protección Datos Personales  
2021-2022

## Integrantes de la Comisión de Protección de Datos Personales

- Brenda Ileana Macías de la Cruz ·  
Aguascalientes
- Lucía Ariana Miranda Gómez ·  
Baja California
- Conrado Mendoza Márquez ·
- Rebeca Lizette Buenrostro Gutiérrez ·  
Baja California Sur
- Rosa Francisca Segovia Linares ·  
Campeche
- Hugo Alejandro Villar Pinto ·
- Marlene Marisol Gordillo Figueroa ·
- Jesús David Pineda Carpio ·  
Chiapas
- Ernesto Alejandro de la Rocha Montiel ·  
Chihuahua
- Laura Lizette Enríquez Rodríguez ·
- Julio César Bonilla Gutiérrez ·  
Ciudad de México
- Luis González Briseño ·  
Coahuila
- Francisco José Yáñez Centeno y Arvizu ·  
Colima
- Alma Cristina López de la Torre · Luz María Mariscal Cárdenas ·
- Paulina Elizabeth Compean Torres ·  
Durango

- José Martínez Vilchis · Guadalupe Ramírez Peña ·  
· Luis Gustavo Parra Noriega · Sharon Cristina Morales Martínez ·

#### Estado de México

- Mariela del Carmen Huerta Guerrero ·

#### Guanajuato

- Francisco Gonzalo Tapia Gutiérrez · Roberto Nava Castro ·

#### Guerrero

- Myrna Rocío Moncada Mahuem · Sigifredo Rivera Mercado ·

#### Hidalgo

- Salvador Romero Espinosa · Natalia Mendoza Servín ·

#### Jalisco

- Areli Yamilet Navarrete Naranjo · Abraham Montes Magaña ·

#### Michoacán

- Roberto Yáñez Vázquez · Hertino Avilés Albavera ·

#### Morelos

- Ramón Alejandro Martínez Álvarez ·  
· Esmeralda Isabel Ibarra Beas ·

#### Nayarit

- María Teresa Treviño Fernández ·  
· María de los Ángeles Guzmán García ·  
· Brenda Lizeth González Lara ·

#### Nuevo León

- María Tanivet Ramos Reyes · Josué Solana Salmorán ·

#### Oaxaca

- Francisco Javier García Blanco ·  
· Harumi Fernanda Carranza Magallanes ·

#### Puebla

- Javier Marra Olea · Alejandra Vargas Vázquez ·

#### Querétaro

- Magda Eugenia De Jesús Lozano Ocman ·

#### Quintana Roo

- José Alfredo Solís Ramírez ·

#### San Luis Potosí

- José Alfredo Beltrán Estrada ·  
· Liliana Margarita Campuzano Vega ·

#### Sinaloa

- Patricia Ordóñez León ·

#### Tabasco

- Didier Fabián López Sánchez ·

#### Tlaxcala

- Aldrin Martín Briceño Conrado ·

#### Yucatán

- Samuel Montoya Alvarez · Fabiola Gilda Torres Rodríguez ·  
· Nubia Coré Barrios Escamilla ·

#### Zacatecas

### **Compilación**

- Elisa Estefanía Contreras Torres ·  
· Anahí Nayeli Prescención Zamudio ·  
· Daniela Castillo González ·

### **Diseño**

- Ernesto González Tapia ·





▶	Presentación.....	1
▶	Prólogo.....	2
▶	<b>00</b> La importancia de un nuevo “ABC de la protección de datos personales”.....	4
▶	<b>01</b> ¿Qué son los datos personales?.....	6
▶	<b>02</b> ¿Conoces los principios rectores de la protección de datos personales?.....	8
▶	<b>03</b> ¿Sabes cuáles son los tipos de datos personales que existen?.....	10
▶	<b>04</b> ¿Sabes qué hay información personal de carácter sensible?.....	12
▶	<b>05</b> ¿Qué es el tratamiento de datos personales?.....	14
▶	<b>06</b> ¿Quién maneja tus datos personales?.....	16
▶	<b>07</b> ¿Cuánta información debemos de dar en algunas oficinas y ante particulares?.....	18
▶	<b>08</b> ¿Sabes cómo se recaban y almacenan tus datos personales?.....	20
▶	<b>09</b> ¿Por qué debes proteger tu información personal al utilizar Internet?.....	22
▶	<b>10</b> Sabes cómo proteger tus datos personales en medios digitales/tecnológicos?.....	24
▶	<b>11</b> ¿Cuáles son los riesgos de compartir tus datos personales?.....	26
▶	<b>12</b> ¿Sabes qué es un aviso de privacidad?.....	28

▶ <b>13</b>	¿Sabes qué son los derechos ARCOP?.....	30
▶ <b>14</b>	¿Conoces la Plataforma Nacional de Transparencia (PNT)?.....	32
▶ <b>15</b>	¿Sabes qué en la PNT puedes realizar solicitudes de derechos ARCOP?.....	34
▶ <b>16</b>	¿Llevas un registro de todos los sitios de internet en donde compartes tu información personal?.....	36
▶ <b>17</b>	3 recomendaciones para un uso responsable y seguro en Internet.....	38
▶ <b>18</b>	¿Cuál es la importancia de la protección de datos personales ante el uso de inteligencia artificial?.....	40
▶ <b>19</b>	¿Sabes qué autoridad en México es la encargada de garantizar el derecho a la protección de datos personales?.....	42
▶ <b>20</b>	¿Conoces la situación actual de la protección de datos personales en México?.....	44
▶ <b>21</b>	Recomendaciones para la Protección de Datos Personales en la infancia y adolescencia.....	46
▶ <b>22</b>	¿Qué hacer ante una vulneración de datos personales?.....	48
▶ <b>23</b>	Las leyes de protección de datos personales en México.....	50
▶ <b>24</b>	¿Qué hacer si las autoridades no responden una solicitud de Derechos ARCOP?.....	52



# PRESENTACIÓN

En los últimos años, el derecho de protección de datos personales se ha constituido como piedra angular para la sociedad de la información; actualmente, se ha hecho común el desarrollo de nuestra vida cotidiana desde la tecnología y la virtualidad. Actividades como la educación, el trabajo, la medicina, el comercio, la recreación y el ocio, ya son una realidad bajo el uso de las Tecnologías de la Comunicación y de la Información (TIC's)

En México, casi el 87 por ciento de las mexicanas y mexicanos son personas usuarias a internet, así lo ha dado a conocer el Instituto Nacional de Geografía y Estadística en la última Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2021; situación que nos lleva a tomar consciencia sobre la relevancia de la adecuada protección de nuestra información personal en el entorno digital.

Ante este panorama, es que desde la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia y Protección de Datos Personales presentamos el **“ABC de la Protección de datos personales”**, como una herramienta que busca, a través de un lenguaje sencillo, el facilitar a la sociedad mexicana el conocimiento de las figuras y conceptos básicos para el ejercicio de este derecho fundamental y, a su vez, tener en cuenta las acciones que se pueden emprender en caso de alguna afectación en la esfera jurídica de las personas.

Sin duda, como integrante de la Comisión de Protección de Datos Personales, representa un gusto poner a disposición del público general un instrumento con el que buscamos fomentar la cultura de protección de datos personales, y mediante el cual también refrendamos el compromiso de los organismos garantes en la contribución para el pleno ejercicio y respeto de la privacidad y la autodeterminación informativa en nuestro país.



# PRÓLOGO

Arístides Rodrigo Guerrero García <sup>1</sup>

<sup>1</sup> Comisionado Presidente del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México y Coordinador de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

La manera en la que la información circula en el siglo XXI es impresionante. En las redes sociales, por ejemplo, tan sólo en un minuto se publican una enorme cantidad de imágenes o videos, en los cuales, se hace referencia a los datos personales, que son aquella información que identifica o hace identificable a una persona,<sup>2</sup> lo que supone importantes riesgos para nuestra privacidad.

La tecnología de nuestros días ha traído consigo una gran cantidad de ventajas. Gracias a ello podemos comunicarnos con las personas desde cualquier parte del mundo, podemos acceder a información muy diversa que facilita la protección de bienes como la salud, como sucedió en la pandemia de COVID-19, en la que a partir de tecnologías como el internet se facilitaba el acceso a la vacunación y a información diversa para evitar y tratar los contagios de esta enfermedad.

<sup>2</sup> Al respecto, uno de los estudios mejor consolidados que dan cuenta del vertiginoso funcionamiento de los entornos digitales es el realizado por la consultora Domo, en el que refieren la cantidad de información transmitida en un minuto a través de internet, como por ejemplo: 575 mil tuits, 167 millones de videos reproducidos en TikTok, 5.7 millones de búsquedas en Google o 65 mil fotografías publicadas en Instagram. Véase: Domo, Data Never Sleeps 9.0. Disponible en: <<https://wAww.domo.com/learn/infographic/data-never-sleeps-9>>.



De la misma manera en que se ha vuelto más cómoda nuestra vida diaria, se han puesto en peligro nuestra privacidad y nuestros datos personales, los cuales, se ha dicho, son el petróleo del siglo XXI, que en caso de ser vulnerados, pueden traer graves consecuencias en la protección de otros bienes como la seguridad, el patrimonio o la vida misma.

Este ABC de la protección de datos personales es un esfuerzo conjunto entre las y los diversos integrantes de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia para socializar y difundir entre la sociedad los aspectos básicos de la PDP a partir de nociones como el significado e importancia de este derecho. Asimismo, en este ABC se han desarrollado con la dimensión práctica de la PDP, tales como su manejo, o almacenamiento, así como importantes referencias a la manera en la que compartimos nuestra información personal en internet.

Por otra parte, se explica el funcionamiento de la Plataforma Nacional de Transparencia y su relevancia para la PDP a la luz de los derechos ARCOP.

Finalmente, podemos encontrar diversas temáticas en las que se explican de manera pedagógica y accesible, cuestiones como las leyes que protegen este derecho y recomendaciones para mantener la seguridad de los datos personales, así como los procedimientos a seguir en caso de una vulneración a la información personal.

Este ABC, integrado por 24 temáticas, busca llegar a diversos sectores de la sociedad para concientizar sobre la importancia de la protección de la privacidad, la cual, tiene implicaciones directas en la construcción de una sociedad democrática y capaz de hacer frente a los retos que impone la incorporación de las cada vez más complejas tecnologías en una gran cantidad de aspectos de la vida cotidiana.

# La **importancia** de un nuevo "ABC de la protección de datos personales"



En las sociedades contemporáneas, es cada vez más común que las personas interactúen utilizando tecnologías de la información y comunicación. Estas interacciones por lo general llevan implícito un intercambio de información personal, tales como la propia imagen, voz, ideas, documentos, entre otros. El entorno digital, como muchos otros instrumentos humanos, si no es utilizado de manera adecuada, en lugar de ser una herramienta útil, puede ser una amenaza para las personas.

El presente "ABC de la Protección de los Datos Personales" se inspira en el esfuerzo de coordinación y colaboración realizado en el marco de la Confederación Mexicana para el Acceso a la Información Pública, al expedir la primera edición del "El ABC de los datos personales", obra editorial pionera en la materia y de gran utilidad para la sociedad mexicana.

Sin lugar a dudas, la reforma constitucional de 2014, es un parteaguas en la garantía del derecho a la protección de datos personales. Desde entonces, el acceso a la información pública y la protección de datos personales

cuenta con organismos garantes constitucionalmente autónomos, uno nacional y treinta y dos de las entidades federativas, que tienen como finalidad el velar por el respeto, promoción, protección y garantía de dichos derechos.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, expedida en 2017, reconoce la conformación de un Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, como una instancia colegiada que tiene la finalidad de establecer las políticas públicas, objetivos, estrategias y acciones de para la protección de datos personales.

Y es a partir de la entrada en vigor de esta Ley General que se incorporan obligaciones específicas para los sujetos obligados, así como atribuciones concretas de los organismos garantes. La necesidad de una obra actualizada precisamente obedece a estos cambios. Por ello, desde la Comisión de Protección de Datos Personales del referido Sistema Nacional, proponemos el “El ABC de la protección de datos personales” como una herramienta de divulgación general sobre conceptos relacionados con los datos personales, la forma en que pueden ejercerse los derechos ARCOP, las particularidades en el funcionamiento de la

Plataforma Nacional de Transparencia respecto a la protección de datos personales, entre otra información de interés.

Para las y los comisionados de los diversos organismos garantes del país que integramos la Comisión de Protección de Datos Personales participar en la elaboración de este instrumento constituye una oportunidad sin igual para orientar a la población. El presente documento es la suma de un cúmulo de experiencias que las y los diversos comisionados consideramos que es indispensable que toda persona conozca y que, mediante un sencillo formato de preguntas y respuestas socializamos la importancia de la protección de datos personales.



# ¿QUÉ SON LOS DATOS PERSONALES?



Información relativa que identifica o hace identificable a una persona.



Informaciones recopiladas que pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.



Datos anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales.

Ambito de aplicación



Recopilación, procesamiento y almacenamiento de datos personales

estrictamente regulado

recopilan, gestionan y almacenan



El uso de los datos personales debe estar documentado e informar claramente a tus usuarios finales.

### Datos personales

Datos que proporcionan cualquier tipo de información. Esta información no debe limitarse necesariamente a la vida privada y familiar de la persona para que entre en el ámbito de los datos personales.

No todos los datos de una persona física se consideran personales. Por ejemplo, los datos anonimizados no se consideran datos personales siempre y cuando no sea posible reidentificar a la persona física a la que se refieren.

# Conoces los PRINCIPIOS RECTORES de la protección de datos personales

Son las **bases y reglas** mediante las cuales los sujetos obligados (SO) deben tratar los datos personales que les confiamos. Cuando exista alguna duda de cómo debe usarse nuestra información personal, debemos en todo momento recurrir a ellos :

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





Los datos deben tratarse con base a las funciones y atribuciones que la ley otorga al SO.



Los datos deben usarse de acuerdo con nuestros intereses.



Los datos deben ser utilizados con intenciones concretas, explícitas, legítimas y lícitas.



Los SO deben mostrarnos un aviso de privacidad en el que nos digan claramente la forma en la que utilizarán los datos que nos piden.



Los SO usarán nuestros datos solo si aceptamos las condiciones que nos expongan. El consentimiento debe ser libre, informado y específico.



Nuestros datos solo pueden ser utilizados si son necesarios, adecuados y relevantes para los fines solicitados.



Los datos que tengan los SO de nuestra persona deben ser exactos, correctos, completos y actualizados.



El SO debe hacer todo lo necesario para que se cumplan con los siete principios anteriores. Asimismo, deben rendir cuentas sobre el uso de nuestros datos.



# ¿Sabes cuáles son los tipos de datos personales que existen?

## Datos de identificación o identificativos:

Nombre y apellidos, imagen, voz, firma autógrafa y electrónica, huella, número de identificación oficial o de pasaporte, clave de elector, número de contribuyente (RFC), clave única de registro de población (CURP), número de cartilla militar, número de tarjeta de residencia, etc.

## Datos relativos a las características personales:

Estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, aficiones y estilos de vida, etc.

## Datos sobre características físicas:

Fisonomía, anatomía y rasgos o particularidades específicas, como: color de la piel, del iris o del cabello; señas y marcas particulares tales como tatuajes, lunares y cicatrices, estatura, peso, compleción, tipo de sangre, ADN, huella digital, registro dental, forma de caminar, tono de voz, entre otras.

## Datos de contacto:

Números de teléfono fijo y móvil, dirección de domicilio, dirección de correo electrónico, etc.

## Datos laborales:

Puesto, empleo, cargo o comisión, denominación de la empresa o institución pública donde se labora, profesión u oficio, desempeño laboral y experiencia laboral, resultados e información relativa a los procesos de reclutamiento, selección, contratación, nombramiento, evaluación y capacitación, correo electrónico institucional, teléfono institucional, referencias laborales, fecha de ingreso y salida del empleo, etc.

## Datos académicos:

Denominación de las instituciones educativas en las que se ha estudiado, formación académica, títulos y certificados académicos, calificaciones, cédula profesional, etc.

### **Datos patrimoniales y financieros:**

Ingresos y gastos, impuestos, rentas, inversiones, créditos y préstamos, número de cuenta bancaria y otros datos bancarios, números de tarjetas bancarias y número de código de seguridad de las mismas, avales, seguros, hipoteca, indemnizaciones, subsidios y beneficios sociales, historial crediticio, bienes muebles e inmuebles, deudas, cargas y obligaciones, etc.

### **Datos relativos a información jurídica:**

Antecedentes penales, las acciones legales ejercidas, las demandas promovidas, los contratos celebrados, los litigios en los que sea parte y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, administrativa o cualquier otra rama del Derecho

### **Datos ideológicos:**

Posturas ideológicas, políticas, religiosas, filosóficas o morales, afiliación sindical, participación en organizaciones civiles, etc.

### **Datos socio-económicos:**

Pertenencia a una comunidad, pueblo, etnia o región, estrato social, origen racial, nivel económico, etc.

### **Datos relativos a vida sexual:**

Orientación, comportamiento, preferencias, prácticas o hábitos sexuales, fotografías íntimas, entre otros.

### **Datos de salud:**

Información relativa a su estado de salud, presente, futura y pasada, historial clínica, enfermedades, tratamientos médicos, alergias, embarazos, estado mental, condición psicológica y/o psiquiátrica, etc.

### **Datos de Datos biométricos: salud:**

Imagen del iris, huella dactilar, palma de la mano u otros análogos.

### **Datos electrónicos:**

Dirección de correo electrónico particular, nombre de usuario, contraseñas, firma electrónica, dirección de IP (Protocolo de Internet) privada, datos de localización (como la función que poseen los teléfonos móviles), cookies, así como cualquier dato relativo al acceso y navegación por internet y que identifique al usuario.

### **Datos de tránsito y movimientos migratorios:**

Información necesaria para el acceso y salida de una persona del país, así como la información necesaria para el tránsito de una persona dentro del mismo. Como ejemplo de ello, podemos señalar los datos personales contenidos en pasaporte, forma migratoria, tarjeta de visitante, tarjeta de residente, etc.



¿ Sabes que hay  
**INFORMACIÓN**  
de **CARÁCTER**  
**SENSIBLE?**



Los datos personales permiten la identificación, localización o autenticación de una persona.



El mal uso de cierta información puede provocar actos de discriminación, segregación o daño sobre la identidad o el patrimonio de su titular.

## Datos personales sensibles:

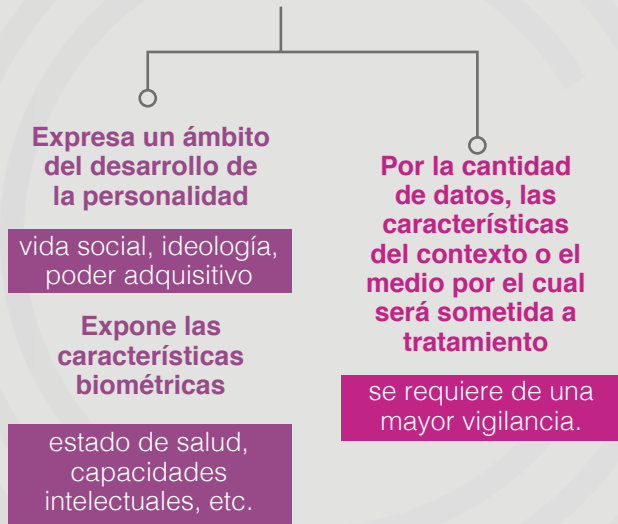
Aquellos que se refieran a la **esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste**. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES  
EN POSESIÓN DE SUJETOS OBLIGADOS

## Información sensible

Debe apegarse de manera más estricta al cumplimiento de los principios regulatorios y sujetarse a mayor cantidad de acciones que promuevan de manera adecuada tanto la integridad de sus soportes, como la confidencialidad por parte de quien la usa.

La información sensible se puede distinguir en dos:





Cuál es el

**TRATAMIENTO**

de **DATOS**  
**PERSONALES?** ...



## Tratamiento de datos personales

Cualquier operación o conjunto de operaciones que se realizan sobre los datos personales cualquiera que sea el tipo de procesamiento (CNIL).



### Tipo de procesamiento

Puede ser definido de manera distinta dependiendo la legislación, el país, la doctrina, etcétera, sin embargo podemos resumirlo a los procesos señalados en la normativa mexicana en materia de protección de datos personales: obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio.

Uso

acceso  
manejo  
aprovechamiento  
transferencia  
disposición de  
datos personales

**Tratamiento  
legitimado**  
(AEPD.2019)



**Principios**

**LICITUD  
FINALIDAD  
CALIDAD  
LEALTAD  
CONSENTIMIENTO  
PROPORCIONALIDAD  
INFORMACIÓN  
RESPONSABILIDAD**

El objetivo o finalidad del tratamiento de los datos, debe ser determinado de manera previa a su obtención





# ¿Quién maneja tus datos personales?

Todo el tiempo los usas y los entregas, de forma tan común, que parece normal: al identificarte en un banco o abordar un avión, al activar un dispositivo electrónico con la huella dactilar, al pagar servicios o compras en línea, al realizar trámites ante alguna institución pública, al usar aplicaciones móviles o incluso al permitir que se genere tu perfil a partir de tus preferencias, en base al historial de navegación o incluso por los “Me gusta” que das en la red, sea imagen, video, historia o publicación y un sinfín de ejemplos más. **¿Cómo identificar, quién es el responsable del manejo de tu información personal?**



Dependerá de  
quién los recaba  
o  
le dará tratamiento:








SI ES  
UNA  
PERSONA  
FÍSICA O MORAL  
DE  
CARÁCTER PRIVADO  
(INCLUYENDO  
SERVICIOS Y VENTAS  
EN LÍNEA), EL  
RESPONSABLE ES:  
UN  
PARTICULAR



« Tu »  
información  
personal



Si es  
alguna  
institución  
pública sea  
de orden  
municipal,  
estatal o  
federal,  
el  
responsable  
es:  
un sujeto  
obligado\*

En ambos casos, **deberán decirte qué, por qué, para qué y quiénes utilizarán tu información**, quién será el responsable de manejar tus datos y cómo ejercer tus derechos ARCOP mediante el aviso de privacidad y hacerlo de tu conocimiento antes de pedírtelos. Si es un sitio electrónico ubicado en el extranjero, tendrá un aviso de políticas de privacidad, revísalo y verifica que no tenga preselección de casillas.

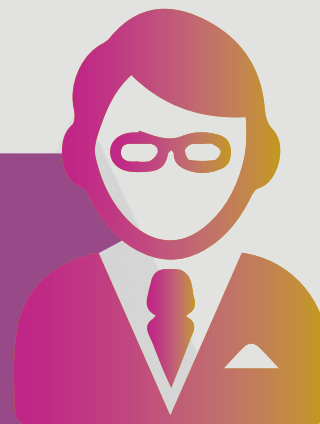
**¡Tú decides a quién le entregas tu información!**

\*Sean del ámbito federal, estatal o municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, organismos autónomos, partidos políticos, fideicomisos y fondos públicos.





# Cuánta información debemos de dar en algunas oficinas y ante particulares





Los datos personales siempre son tuyos, pero a veces es necesario que los proporciones a otros para hacer un trámite (oficinas de tránsito, escuelas, hospitales públicos, tribunales, procuradurías, entre otros), de igual forma al comprar un producto o contratar un servicio a particulares (médicos, bancos, hoteles, empresas de telefonía móvil, aseguradoras, etc).

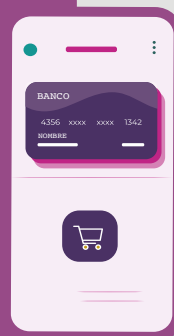


Las entidades públicas y privadas deben cumplir con la normativa y, además, ser capaces de demostrar dicho cumplimiento mencionado en su aviso de privacidad, el cual tiene como propósito principal hacer del conocimiento del Titular de los datos personales que su información personal será recabada y utilizada para ciertos fines, y las características del tratamiento al que serán sometidos sus datos personales.



Los responsables del tratamiento de tus datos personales solo te deberán solicitar aquellos datos que resulten necesarios, adecuados y relevantes para cumplir con las finalidades para las cuales se obtuvieron, y además deberán procurar solicitarte el menor número posible de datos personales.

# ¿Sabes cómo se recaban y almacenan los datos personales?



Cuando realizas un trámite o compras algún producto o servicio, muchos datos personales son recabados y después utilizados, aprovechados y almacenados en distintos medios o soportes.

## Tipo de soportes: físicos y electrónicos

### SOPORTES ELECTRÓNICOS

Requieren de algún aparato que procese su contenido.



Almacenamiento en la nube

Unidad de Disco Duro

Discos ópticos (CD/DVD)

Memoria USB

Discos magnéticos



### SOPORTES FÍSICOS

Medios de almacenamiento que no requieren ningún aparato para ser procesados.



Documentos

Oficios

Formularios impresos

Fotografías

Placas radiológicas

Carpetas

Expedientes

# ¿Por qué debes PROTEGER TU INFORMACIÓN PERSONAL al utilizar INTERNET?



Luis Gustavo Parra Noriega

INTERNET

**PUBLICAR** | pensamientos, fotos o vídeos

**INFORMAR** | de lo que acontece en cualquier parte del mundo a solo unos segundos de haberse dado los acontecimientos

**ENTRETENER** | a través de los servicios de streaming para ver series y películas, escuchar música y jugar video juegos, incluso es posible comprar a través de diversas plataformas de comercio electrónico.

**INTERACTUAR** | con otras personas a miles de kilómetros de distancia

## EL LIMITE DEL INTERNET ES LA PROPIA CREATIVIDAD DE LAS PERSONAS



Ha permitido extender nuestra humanidad a un plano que sin ser físico impacta en todos los aspectos de nuestra vida.

Resulta fundamental tener cuidado con la forma de conducirnos en el plano virtual que ofrece Internet

El anonimato que permite la red y la facilidad con que es posible deshumanizar la interacción que se desarrolla en ésta, puede traer consigo la comisión de conductas reprobables como lo son el acoso, la discriminación, la misoginia, la xenofobia e incluso delitos cibernéticos.

Es importante tener conciencia que cada vez que usamos esta red, sin importar la plataforma en la que estemos navegando, se almacenan datos que pueden aportar desde rutinas o hábitos de los usuarios, hasta la identificación de datos sensibles de las personas, a través del uso de tecnología y algoritmos.

**Acceder al conocimiento y la información que aporta Internet, sin perder de vista el cuidado de la privacidad y la protección de nuestros datos personales.**

Para lograrlo es necesario el empoderamiento de los usuarios para el uso ético de estas tecnologías, con base en el fortalecimiento de la cultura de la protección de datos personales, la privacidad y el ejercicio de la autodeterminación informativa.



¿  
SABES CÓMO  
PROTEGER  
TUS DATOS  
PERSONALES  
EN MEDIOS  
DIGITALES /  
TECNOLÓGICOS?  
!



## GLOBALIZACIÓN Y LA MASIFICACIÓN DEL ACCESO AL INTERNET Y LAS TICS



Ha dado pie a nuevos escenarios y desafíos en el tema de las violencias, las violaciones y atropellos al Derecho de Protección de Datos Personales, en especial hacía ciertos grupos que ya tienen un largo historial de vulnerabilidad sociohistórica. La intimidad de las y los mexicanos nunca había estado tan expuesta y al alcance. Muchos de estos datos personales también tienen un alto valor económico en el mercado y se vuelven susceptibles de utilizarse para la comisión de un delito.

### “FRADES CIBERNÉTICOS TRADICIONALES”

de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

### QUEJAS POR FRADES CIBERNÉTICOS

tercer trimestre

2019

+

38%

respecto de 2018

La tecnología ha permitido mantener cercanía, continuar con la actividad laboral y escolar en medio de una pandemia, entre otras bondades. Pero al mismo tiempo, tan solo por mencionar un evento lamentable, ha recrudecido la violencia de género digital.

La **portabilidad de datos no consentida** ha ido en aumento, el manejo de celulares inteligentes, la navegación en páginas web no seguras, las múltiples redes sociales, el uso de aplicaciones en los teléfonos inteligentes, la exposición al compartir datos en videojuegos en línea, las reuniones virtuales en plataformas, etc; son algunos de los espacios virtuales en los que más expuestos están nuestros Datos Personales, por ello es de vital importancia leer los avisos de privacidad, cuestionarse si es necesario compartir nuestra información y sobre todo, valorar la utilidad de estos medios tecnológicos de comunicación, precisando que, es necesario observar y vigilar lo que las y los menores de edad consumen en estos espacios, así como leer y familiarizarse con las guías que el INAI y los órganos garantes han puesto a nuestro alcance para una navegación segura, son tan solo algunas de las cosas que podemos hacer para cuidarnos entre todas y todos.



# Cuáles son los riesgos de compartir tus datos personales?

Hugo Alejandro Villar Pinto



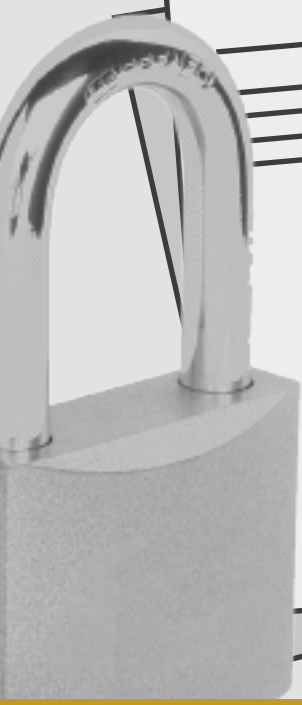
Las redes sociales, las nuevas tecnologías y la globalización, representan una importante herramienta para mantenernos informados en tiempo real, tienen al mismo tiempo, consecuencias positivas y negativas, lo que significa la existencia de riesgos que afectan directamente, sobre todo a las niñas, niños y adolescentes, no obstante, todas las personas estamos expuestos en el mundo digital y físico.

Existen diversos riesgos y peligros reales que no visualizamos, entre ellos el robo de identidad, el robo a casa habitación, secuestro, pornografía, trata de personas, acoso o ciberbullying, extorsión, fraude, falsificación, daño a la moral, entre otros delitos que son cometidos no solo desde la realidad virtual, sino también desde la física, a partir de información que exponemos en la red.

El uso de la tecnología en la vida cotidiana ha permitido que muchas actividades trámites y gestiones se realicen por medio de equipos electrónicos que contienen gran parte de nuestra información personal, por ello es recomendable cambiar las contraseñas periódicamente y procurar que sean contraseñas seguras, cuidando los códigos de seguridad, es decir, que incluyan mayúsculas, minúsculas, números y símbolos, así como utilizar una contraseña distinta en cada cuenta importante, garantizando un nivel más óptimo de seguridad.

Es obligación de las Instituciones proteger los datos personales y coadyuvar en el fomento de una cultura de protección de los datos personales, garantizando que no serán utilizados con fines distintos para los cuales fueron proporcionados, previniendo la afectación de derechos, libertades y sobre todo, protegiendo y salvaguardando la dignidad de las personas.

**¡Porque nuestros datos  
personales valen!**



¿Sabes que es un **AVISO** de **PRIVACIDAD?**



Las Instituciones, públicas o privadas, tienen la obligación de poner a disposición de los titulares de los datos personales, un documento que se denomina Aviso de Privacidad.

## OBJETIVO

informar al titular, las generalidades del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones de manera informada.

El Aviso de Privacidad, deberá contener de manera enunciativa, más no limitativa, la siguiente información:

La denominación y el domicilio del responsable;

Los datos personales recabados;

El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;

En su caso, las transferencias;

Las finalidades del tratamiento;

Los mecanismos, medios y procedimientos disponibles para ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO), y

Los procedimientos a través de los cuales, el responsable comunicará a los titulares, los cambios al Aviso de Privacidad.

El Aviso de Privacidad, se puede poner a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable.



DE  
RE  
CHOS

ARCOP

Son una garantía del derecho de autodeterminación de las personas como titulares de datos personales que les permiten mantener el control y disponer de sus datos personales frente a los responsables pertenecientes del sector público o privado .

## **A**cceso

Derecho de Acceso: Es la facultad de solicitar el acceso a los datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes de los responsables, que los almacena o utiliza, así como conocer la información relacionada con las condiciones y generalidades del tratamiento que se les da.

---

## **R**ectificación

Derecho de Rectificación: Es la facultad de solicitar a cualquier responsable la corrección de los datos personales que posean derivados de un trámite o servicio realizado, y estos sean inexactos o incompletos o no se encuentren actualizados.

---

## **C**ancelación

Derecho de Cancelación: Es la facultad de solicitar que los datos personales sean suprimidos o eliminados de los archivos, registros, expedientes, sistemas, bases de datos de cualquier responsable y dejen de ser tratados. En algunas ocasiones no podrá ejercerse este derecho cuando los datos personales estén sujetos a cumplimientos legales.

---

## **O**posición

Derecho de Oposición: Es la facultad de solicitar a cualquier responsable que se abstenga de utilizar información personal para ciertos fines, por ejemplo, la publicación de datos personales en alguna fuente de acceso público, o de requerir que se concluya el uso de los mismos a fin de evitar un daño o afectación. En algunas ocasiones no podrá ejercerse este derecho cuando los datos personales estén sujetos a cumplimientos legales.

---

## **P**ortabilidad

Derecho de Portabilidad: La portabilidad consiste en el derecho que tienen las personas, para requerir a quien se encuentra dándole tratamiento a sus datos personales en un formato electrónico estructurado y de uso común, que obtenga una copia y/o transfiera a otro responsable que le indique la persona titular.

# ¿Conoces la PNT?

Es el espacio en el que puedes consultar todo lo que producen o resguardan las instituciones públicas de México, y es también el medio para solicitarles información.



## **SIPOT** | Sistema de Obligaciones de Transparencia

Es una herramienta electrónica a través de la cual los Sujetos Obligados, ponen a disposición de las personas la información que poseen y generan en cumplimiento a las obligaciones de transparencia contenidas en la Ley General, Ley Federal o Ley Local y en los Lineamientos Técnicos Generales para la publicación, homologación y estandarización de las obligaciones.

## **SISAI** | Sistema de Solicitudes de Información

Permite a las personas requerir a los Sujetos Obligados de los tres órdenes de gobierno, información pública de su interés, así como el acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, asimismo permite a los Sujetos Obligados gestionar los requerimientos de información en los términos y plazos que establecen la Ley General, Ley General de Datos y las respectivas Leyes locales en la materia.

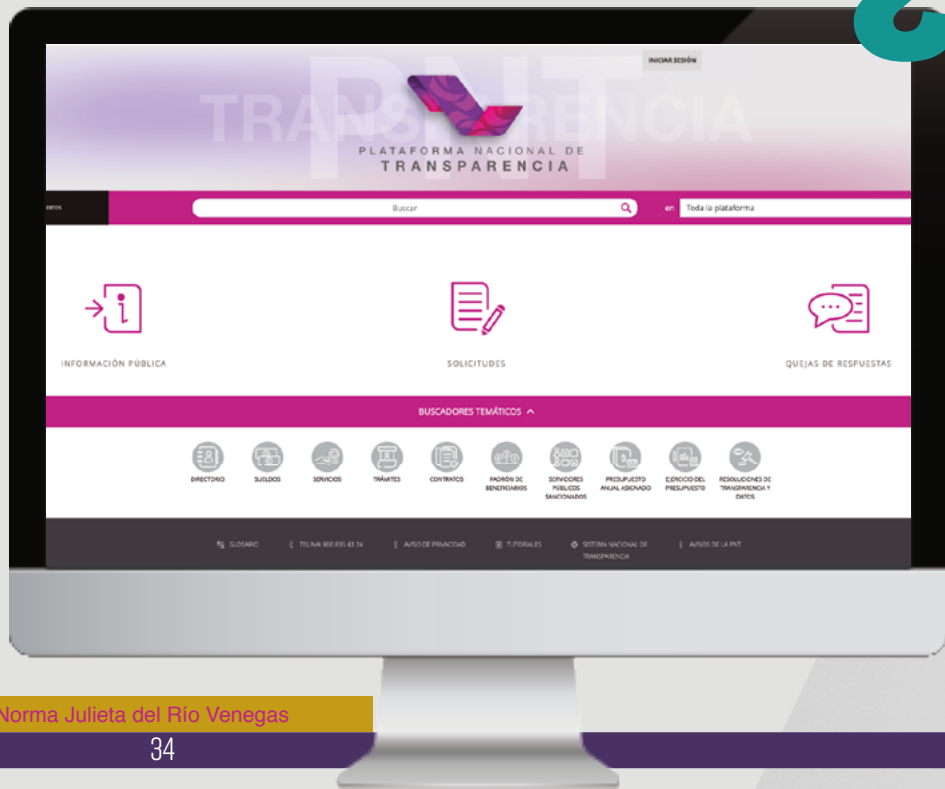
## **SIGEMI** | Sistema de gestión de medios de impugnación

El SIGEMI permite a las personas interponer recursos de revisión (quejas) ante los Organismos Garantes, por inconformidad con la respuesta o por la falta de ésta, a solicitudes de información y ARCOP de parte de los Sujetos Obligados, así como dar el seguimiento correspondiente.

## **SICOM** | Sistema de comunicación entre organismos garantes y sujetos obligados

Permite la comunicación entre el Organismo Garante con sus respectivos Sujetos Obligados para realizar las actuaciones de los recursos de revisión interpuestos por las personas, conforme la Ley General, Ley General de Datos y las leyes y procedimientos locales en la materia, asimismo permite a los Organismos Garantes gestionar los recursos de revisión y a los Sujetos Obligados atender las notificaciones o requerimientos que se les haga, en tiempo y forma.





# Sabes que en **la PNT** puedes realizar solicitudes de los derechos **ARCOP**?

La Plataforma Nacional de Transparencia te permite ejercer tu derecho de protección de datos personales, para esto puedes realizar una solicitud por medio de ella, aquí te enseñamos como:



## INGRESO

Para generar una solicitud deberás ingresar con una cuenta válida en la PNT.

## CAPTURA

Para generar tu solicitud deberás capturar la información de los campos requeridos, así como aceptar el aviso de privacidad.

**SOLICITUD DE PROTECCIÓN DE DATOS PERSONALES (ARCOPI)**

Los campos marcados con (\*) son obligatorios

¿Quién presenta la solicitud?

Datos del titular

Nombre(s)\*

Primer Apellido  Segundo Apellido

Tipo de derecho\*

Denominación de la institución a la que solicitas información\*

Estado o Federación

Institución

**Solicitud de Datos Personales**

Detalle de la solicitud\*

Leí el Aviso de Privacidad y otorgo el consentimiento para que mis datos personales sean tratados conforme al aviso de privacidad.

ENVIAR

## ACUSE

Por último, te dará un acuse que comprueba el ingreso de tu solicitud así como la fecha de respuesta para tu solicitud.

Se han creado las siguientes solicitudes de información

Acuse Folio Estado o Federación

3134243546 Federación

ACEPTAR

[www.plataformadetransparencia.org.mx](http://www.plataformadetransparencia.org.mx)



# Llevas un registro de todos los sitios de Internet en donde compartes tu información personal ?

El internet ha sido una herramienta transformadora en nuestras vidas, que ha simplificado muchos procesos que llevamos a cabo de manera cotidiana y nos ha permitido permanecer conectados unos con otros con mayor facilidad.

Sin embargo, al navegar a través del internet, en las diferentes plataformas y aplicaciones informáticas que existen, como son: las redes sociales, las páginas web, la banca por internet, las tiendas en línea, las plataformas de streaming y diversas aplicaciones, en las que sin darnos cuenta vamos compartiendo nuestra información personal, lo que puede conllevar algunos riesgos.

Es así, como el **internet resulta beneficioso** para muchas de las actividades que realizamos, pero la información que vamos dejando al visitar los diversos sitios, puede ocasionarnos una **vulneración a nuestra privacidad**, podemos ser víctimas de robos de identidad, recibir ataques de códigos maliciosos que pueden secuestrar nuestra información, entre otros delitos cibernéticos.

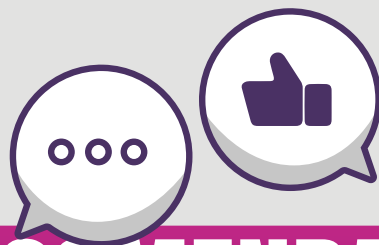


Bajo este contexto como usuarios de la red, es importante **mantener un control de los sitios que visitamos**, atendiendo las siguientes recomendaciones:

- Antes de proporcionar los datos personales, leer los Avisos y/o Políticas de Privacidad que garanticen la confidencialidad de la información.
- Llevar un registro de los sitios web en los que se han ingresado Datos Personales.
- Verificar las finalidades por las que se tratan los datos personales y si existirán transferencias de datos con otros responsables.
- Crear contraseñas en todos los dispositivos.
- Limitar la información personal que se comparte en redes sociales.

Fuentes consultadas:

<https://staysafeonline.org/blog/7-tips-to-manage-your-identity/>  
<https://www.legalzoom.com/articles/8-smart-ways-to-protect-your-personal-data>  
<https://www.mebank.com.au/the-feed/7-ways-to-protect-your-digital-privacy/>



# 3 RECOMENDACIONES

## PARA UN USO RESPONSABLE Y SEGURO EN INTERNET



1

### Protege tu integridad.

Restringe el acceso a lo que publicas en tus redes sociales y autoriza que accedan sólo a quienes conozcas. Tampoco compartas fotos o información íntima en Internet.

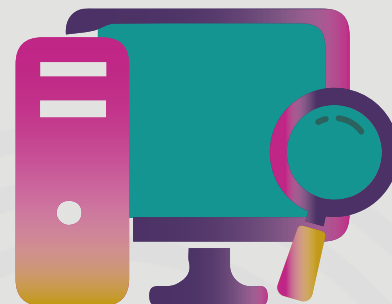
**Recuerda que lo que publicas en Internet se queda grabado por siempre y puede ser usado por otras personas para dañarte a ti o a los tuyos.**



2

## Protege tu información.

Genera contraseñas largas que combinen números, letras y signos especiales, así reducirás el riesgo de que alguien las descifre y entre a tus perfiles y cuentas. Además, modifícalas periódicamente. Evita usar contraseñas prediseñadas por programas y cierra tus sesiones siempre que salgas de tus sitios web.



3

## Protégete tus datos en la tecnología.

Compra en portales online que tengan el ícono del “candadito” en su dirección web. Ello significa que son sitios seguros donde tus datos se manejan de manera cifrada.

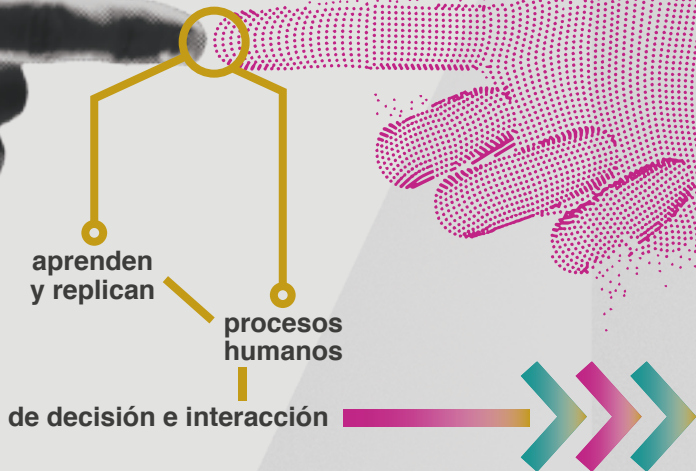
No utilices servicios de Wi-Fi públicos ni programas gratuitos o libres, ya que carecen de las seguridades para proteger tu información de los ciberdelincuentes.

Evita abrir mensajes de desconocidos o que te ofrezcan productos gratuitos. Recuerda que, **si te ofrecen algo “gratis”, ¡tus datos son el precio a pagar!**





■ Cuál es la importancia  
de la **PROTECCIÓN  
DE DATOS  
PERSONALES**  
ante el uso de **INTELIGENCIA  
ARTIFICIAL** ?





Han dado forma a los servicios de usuario actuales, lo que permite, por un lado, una mejor personalización y mejor soporte. Como tales servicios basados en IA inevitablemente requieren datos de las y los usuarios, estos representan riesgos en su tratamiento, manejo, transferencia y seguridad y, consecuentemente, para la autodeterminación informativa, intimidad, privacidad y dignidad de las personas.

Por ello, el uso de IA y sus algoritmos en técnicas modernas y automatizadas de procesamiento y análisis de datos, así como las tendencias tecnológicas intensivas en su uso, sugieren la necesidad de que todas y todos, personas e instituciones, adoptemos una visión más amplia acerca de su impacto en la protección de los datos de las personas. Sobre todo porque estas herramientas de IA han avanzado hasta el punto de tener la posibilidad de predecir las actuaciones, gustos e intereses de las personas, a partir de los datos que compartimos y se someten a su análisis, muchas veces sin el conocimiento ni mucho menos la autorización del titular de estos datos.

En ese contexto, es de la mayor importancia que las personas, protejamos nuestros datos personales, no los compartamos y nos informemos debidamente, acerca del tratamiento, uso y destino que cualquier servicio digital dará a los mismos.





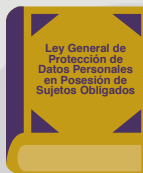
inai

¿ SABES QUE  
**AUTORIDAD**  
EN **MÉXICO** ES LA  
**ENCARGADA**  
DE **GARANTIZAR**  
EL **DERECHO**  
A LA **PROTECCIÓN**  
DE **DATOS**  
**PERSONALES?**





En México, como en muchos otros países, es importante considerar que el derecho a garantizar la protección de datos personales se encuentra previsto en distintas regulaciones, según el ámbito de competencia del que se trate.



En el sector público, existe la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que regula el tratamiento de datos personales por parte de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal, estatal y municipal. La cual faculta al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales para su aplicación y tutela en toda la nación.



De manera adicional, cada entidad federativa cuenta con una ley específica que detalla las disposiciones que regulan el tratamiento de datos personales en el sector público estatal y municipal, misma que se encuentran armonizadas con la Ley General, facultando a los Órganos Garantes Locales para su aplicación en el ámbito de sus competencias.




Entre las diversas facultades que emanan de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el INAI garantizará el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados, conociendo y resolviendo los recursos de revisión y de inconformidad, desarrollando los procedimientos de verificación para su cumplimiento, así como ejecutar medidas de apremio.



Por otro lado, contamos con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que regula el tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas, facultando al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales para su aplicación en todo el territorio nacional sobre personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales.

Cámara de Diputados. (26 de enero de 2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Diario Oficial de la Federación.



# ¿Conoces la situación actual de la protección de datos personales en México?

Actualmente, México se encuentra entre los países que tienen reconocida la protección de los datos personales como un derecho fundamental. De hecho, **nuestro país posee una regulación avanzada y rigurosa** en materia de protección de datos personales, semejante a las existentes en Europa y en otros países de Latinoamérica.

El **artículo 16**, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos consagra el derecho humano a la protección de los datos personales. Ahora bien, en México existe una peculiaridad que consiste en que tenemos dos legislaciones en materia de protección de datos personales con un ámbito subjetivo de aplicación distinto.



Por un lado, tenemos la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la cual fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010. Esta normativa aplica al tratamiento de datos personales llevado a cabo por particulares, es decir, personas físicas o jurídicas de carácter privado. Por ejemplo, son sujetos regulados por esta Ley, entidades bancarias, compañías de seguros, fianzas y coaseguros, compañías proveedores de servicios de telefonía e internet, etc.




Por otro lado, se tiene una normativa que aplica al sector público, es decir, al tratamiento de datos personales llevado a cabo por autoridades (entre otros sujetos) del orden federal, estatal y municipal. En este rubro, se encuentra la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual fue publicada en el Diario Oficial de la Federación el 26 de enero de 2017. Asimismo, cada Entidad Federativa cuenta con la facultad constitucional para emitir su propia normativa en materia de protección de datos personales, aplicable al sector público estatal, la cual debe estar ajustada a las disposiciones de la citada Ley General.

De forma más reciente, el 12 de junio de 2018, México se adhirió al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio N° 108 del Consejo de Europa) y, de igual manera, al Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, mismos que constituyen unos instrumentos jurídicos en la materia de protección de datos personales que tienen vocación universal, ya que están suscritos por 53 países de todo el mundo.



Con todo ello, se puede afirmar que nuestro país se encuentra comprometido con la protección de la información personal de sus ciudadanos. Sin embargo, actualmente se está buscando ampliar el alcance de la normativa vigente en la materia, para adaptarla a la era digital.




# RECOMENDACIONES PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA INFANCIA Y ADOLESCENCIA



67.1%

de niñas y niños entre 6 y 12 años de edad tienen acceso a internet.



38.4%

de la población infantil cuentan con un dispositivo con el que pueden comunicarse, interactuar y acceder a información a través de internet.

## #PDP

de la niñez asume una gran importancia, la vida privada es un valor indispensable en las sociedades democráticas, representa un auténtico límite al poder del Estado y al de las organizaciones privadas.

## VULNERACIÓN

acciones de difusión y apropiación indebida de la información que identifica o vuelve identificable.

Fenómenos que vulneran los datos personales y la privacidad de niñas y niños en el entorno virtual:



### Sharenting

Publicación excesiva en redes sociales de imágenes de menores por parte de los padres, que compromete a la privacidad y el derecho a la identidad de niñas y niños.



### Cyberbullying

Acoso producido entre niñas y niños a través del uso de internet en redes sociales.



### Sexting

A través de plataformas de mensajería se intercambian fotografías o videos con connotación sexual.



### Vishing

Estafa a través de una conversación en la que suplantan la identidad de una persona de confianza.



### Grooming

Un adulto establece amistad con niñas, niños o adolescentes a través de internet con la finalidad de obtener imágenes o vídeos con contenido sexual.



### Violencia digital

Actos de agresión basados en la desigualdad de género llevados a cabo mediante el uso de las tecnologías de la información.

Para garantizar la máxima protección de los datos personales de las infancias, se recomienda:



Limitar la descarga de aplicaciones o juegos sin autorización.



Utilizar adecuadamente las configuraciones de privacidad.



Usar contraseñas seguras.



Evitar la difusión de fotografías y videos en el que se aprecie claramente el rostro de niñas y niños.



¿Qué hacer en caso de una

# VULNERACIÓN de datos personales?



En el 2021, México tuvo más de 156 mil millones de intentos de ciberataques, según Fortinet.



**Pérdida o destrucción**  
no autorizada



**El robo, extravío o copia**  
no autorizada



**El uso, acceso o tratamiento**  
no autorizado



**El daño, la alteración o modificación**  
no autorizada

ANTE CUALQUIER  
VULNERACIÓN  
**ACUDE** AL INSTITUTO  
NACIONAL DE  
TRANSPARENCIA,  
ACCESO A LA  
INFORMACIÓN Y  
PROTECCIÓN DE  
DATOS PERSONALES,  
O AL ÓRGANO G  
ARANTE DE TU  
ENTIDAD FEDERATIVA  
QUE CORRESPONDA.



Las  
**Leyes**  
de  
**protección**  
de  
**DATOS**  
**PERSONALES**  
en **México**

## DATOS PERSONALES

“Cualquier información concerniente a una persona física identificada o identificable”

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

“Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información”

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



**Generar información** forma parte sustancial y permanente de las personas. Vivimos constantemente en el proceso de establecer y formular información.

Se ha de determinar la concepción de los datos personales establecida en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) como “cualquier información concerniente a una persona física identificada o identificable”.

La Ley General de la Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) , formaliza el concepto como la esencia de las leyes mencionadas (LFPDPPP & LGPDPPSO).

Lo que motivó a los legisladores de México para integrar el sustantivo (protección), en la esfera jurídica es notoriamente la inseguridad y el interés por garantizar el cuidado de la información de carácter personal de la ciudadanía mexicana.

La LGPDPPSO establece en su **artículo 6** que el **Estado debe de garantizar la privacidad de los individuos y destaca las obligaciones del Estado mexicano en favor de la protección de los Derechos Humanos.** El Derecho a la protección de Datos Personales, constituye un instrumento jurídico vital para el progreso de la sociedad, constituyendo un derecho subjetivo, perteneciente a la tercera generación, relacionado con lo dispuesto en el artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos.

Lo dispuesto en las leyes faculta e informa a las personas para decidir y controlar con libertad las condiciones en las cuales serán utilizados sus datos personales.



¿ QUÉ HACER SI LAS  
AUTORIDADES  
**NO**  
**RESPONDEN**  
UNA SOLICITUD DE  
**DERECHOS**  
**ARCOP?**



**Presentar un Recurso de Revisión**, el cual es un medio de defensa con el que cuentan las personas para manifestar su inconformidad ante la respuesta a la solicitud otorgada o la falta de esta, por parte de las autoridades del ámbito federal, estatal o municipal.



Se deberá presentar ante el INAI o el órgano garante estatal que corresponda, dentro de los 15 días hábiles siguientes a la fecha en que se haya vencido el plazo que tenía la autoridad para emitir la respuesta y no lo hizo, o que entregándola exista inconformidad con ella.



Los medios para presentar el recurso de revisión son:



Escrito libre en el domicilio de los órganos garantes del país o el INAI.



Correo certificado.



Correo electrónico.



Plataforma Nacional de Transparencia  
[www.plataformadetransparencia.org.mx](http://www.plataformadetransparencia.org.mx)

Es importante señalar en la inconformidad: el área ante la que se presentó la solicitud, nombre del titular, fecha de notificación de la respuesta o de la presentación de la solicitud, el acto y motivos de inconformidad, en su caso copia de la respuesta, y los documentos que acrediten que eres el titular de los datos personales, o el de tú representante legal.



**SISTEMA NACIONAL  
DE TRANSPARENCIA**

ACCESO A LA INFORMACIÓN PÚBLICA  
Y PROTECCIÓN DE DATOS PERSONALES



**COMISIÓN  
DE PROTECCIÓN  
DE DATOS PERSONALES**