GUÍA ORIENTADORA

“La protección de Datos Personales en plataformas digitales”

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

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

COMISIÓN DE PROTECCIÓN DE DATOS PERSONALES

Construyendo Transparencia 15 años Info Ciudad de México

GUÍA ORIENTADORA

"La protección de Datos Personales en plataformas digitales"

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

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

Comisión de Protección de Datos Personales

Construyendo Transparencia
15 años
Info Ciudad de México

Av. Insurgentes Sur No. 3211, colonia Insurgentes Cuicuilco, alcaldía Coyoacán, Ciudad de México. C.P. 04530.

Primera edición: octubre de 2021

Directorio

Blanca Lilia Ibarra Cadena
Comisionada Presidenta del INAI y del SNT

Francisco Javier Acuña Llamas
Comisionado del INAI

Adrián Alcalá Méndez
Comisionado del INAI

Norma Julieta del Río Venegas
Comisionada del INAI

Oscar Mauricio Guerra Ford
Comisionado del INAI

Rosendoevgueni Monterrey Chepov
Comisionado del INAI

Josefina Román Vergara
Comisionada del INAI

Coordinadores

Cinthya Denise Gómez Castañeda
Coordinadora de la Comisión de Protección de Datos Personales del SNT

Arístides Rodrigo Guerrero García
Secretario de la Comisión de Protección de Datos Personales del SNT

Laura Lizette Enríquez Rodríguez
Comisionada del INFO CDMX

Colaboradores

Luis Gustavo Parra Noriega

Myrna Rocío Moncada Mahuem

Alma Cristina López de la Torre

Laura Lizette Enríquez Rodríguez

Samuel Montoya Álvarez

Areli Yamilet Navarrete Naranjo

Luis González Briseño

María Elena Guadarrama Conejo

María Antonieta Velásquez Chagoya

Josefina Román Vergara

María Teresa Treviño Fernández

Liliana Margarita Campuzano Vega

Arístides Rodrigo Guerrero García

Norma Julieta del Río Venegas

Lucía Ariana Miranda Gómez

Equipo de Trabajo de la SESNT

Federico Guzmán Tamayo
Secretario Ejecutivo del SNT

María Teresa González Corona
Subdirectora de Seguimiento A de la SESNT

Janeth Vázquez Reyes
Subdirectora de Seguimiento B de la SESNT

María Guadalupe Manjarrez Segura
Asesora de la SESNT

Paula Angélica Lomelí Cázares
Enlace de la SESNT

Equipo de Trabajo de la Comisión de Protección de Datos Personales

Daniel Humberto Nuñez Valadez
Proyectista A

Anahí Nayeli Prescención Zamudio
Auxiliar de Pleno

Esther Elizabeth Albarrán Martínez
Asesora de Ponencia

Equipo de Trabajo de la DGVCCEF

José Luis Naya González
Director General de Vinculación, Coordinación y Colaboración con Entidades Federativas

María Elena Vázquez Reyes
Directora de Vinculación y Coordinación con Entidades Federativas

Prólogo

El siglo XXI es el siglo de la era digital. Una era donde la especialización del conocimiento, los avances tecnológicos a gran escala y la automatización de los procesos de producción han provocado profundas transformaciones en distintos ámbitos y niveles. Por ejemplo, de acuerdo con la Organización de las Naciones Unidas, en apenas 20 años, las tecnologías digitales han llegado a cerca del 50% de la población del mundo en desarrollo, mejorando la conectividad, la inclusión financiera, las actividades comerciales o la oferta de servicios públicos[1]. De esta manera, las nuevas tecnologías, según apunta el organismo internacional, constituyen una vía poderosa para construir un mundo más equitativo, justo y sostenible.

Asimismo, la Comisión Económica para América Latina y el Caribe (CEPAL), puntualizó el impacto sistémico traído por la disrupción digital, con la integración a nuestras actividades de nuevos dispositivos y aplicaciones tecnológicas —como el cómputo en la nube, la inteligencia artificial, la cadena de bloques, entre otros—, que han generado un nuevo modelo económico donde los bienes y servicios adquieren un valor añadido, gracias a la reducción de los costos de transacción y el aprovechamiento de la información que se obtiene del análisis de los datos que se generan e intercambian de forma masiva en las plataformas digitales[2].

Sin embargo, el auge de la denominada "Cuarta Revolución Industrial" también ha provocado una serie de efectos adversos para la sociedad. Éstos incluyen desde la prevalencia de una brecha digital que relega a una proporción importante de la población de los beneficios de la digitalización —puesto que carecen de habilidades y competencias para usar las herramientas digitales— hasta la propagación de información falsa, la

1 ONU (2021) "Influencia de las tecnologías digitales", Naciones Unidas, Disponible en: https://www.un.org/es/un75/impact-digital-technologies

2 CEPAL (2021) "Tecnologías Digitales para un Mejor Futuro", CEPAL: Santiago, Disponible en: https://www.cepal.org/es/publicaciones/46816-tecnologias-digitales-un-nuevo-futuro

exposición a ciberataques, la segmentación de perfiles, la manipulación de comportamientos y la vulneración de prerrogativas fundamentales, como el derecho a la privacidad o a la protección de datos personales.

Este último punto es de la mayor relevancia, pues según el Informe de Economía Digital 2021, de la Conferencia de las Naciones Unidas Sobre Comercio y Desarrollo, la pandemia de COVID-19 y las medidas de distanciamiento físico aceleraron el proceso de transformación digital, al privilegiar los canales remotos para la realización de diversas actividades3

Tal situación, no solo consolidó el potencial disruptivo que ofrece la era digital, con el uso estratégico de los datos para la generación de nuevas cadenas de valor y relaciones comerciales, la modernización en la provisión de servicios o la participación ciudadana en la atención de problemas públicos de diversa índole; sino que también amplió las posibilidades de que, ante un tratamiento y flujo intensivo de datos e información, se presenten una serie de amenazas como su recopilación y transferencia no autorizada, la concreción de actividades ilegales o la afectación a ciertos derechos y libertades.

La gobernanza, el aprovechamiento y la adecuada seguridad de la gran cantidad de datos que circulan en las plataformas digitales vuelve impostergable armonizar las bondades del progreso tecnológico con la protección de los usuarios, desplegando marcos regulatorios y acciones de capacitación que permitan la transferencia de información con estándares de seguridad apropiados para la garantía de los derechos humanos.

Con este marco de referencia, desde el Sistema Nacional de Transparencia (SNT) se ha generado esta Guía Orientadora: *"La protección de datos personales en plataformas digitales"*, un instrumento que busca exponer las principales problemáticas en torno a la información personal que se comparte en las plataformas digitales, que además contó con la participación de las comisionadas y los comisionados que integran la Comisión de Protección de Datos Personales del SNT, quienes aportaron su conocimiento, su experiencia y su profesionalismo para desarrollar este documento. La Guía ofrece al lector una valiosa herramienta que ofrece y explica una lista de 17 temáticas formuladas a manera de cuestiona-

3 UNCTAD (2021) "Informe de Economía Digital 2021", Naciones Unidas, Disponible en: https://unctad.org/system/files/official-document/der2021_en.pdf

mientos, que estimulan la reflexión en torno a temas que van desde la protección de datos personales, las plataformas e identidades digitales, o el aviso de privacidad, hasta las evaluaciones de impacto a la privacidad y la legislación aplicable en la materia.

Sin duda, todavía falta mucho camino por recorrer en la difícil tarea de garantizar que el desarrollo tecnológico contribuya a generar mayores condiciones de igualdad en favor de las personas, las comunidades y el respeto de los derechos humanos. No obstante, desde el Sistema Nacional de Transparencia estamos convencidos de que, precisamente, con acciones de promoción y socialización de los derechos que tutelamos desde los Organismos Garantes del país, será más sencillo fortalecer el desarrollo de una cultura de privacidad y cuidado de la información personal, ante un escenario en donde las plataformas digitales son ya un elemento insustituible del progreso global.

Por todo lo anterior, no queda más que celebrar la materialización de esta Guía Orientadora, pues ha puesto de manifiesto, nuevamente, la labor de los Organismos Garantes y del Sistema Nacional de Transparencia en favor del respeto y la promoción de los derechos de las personas como una vía que apuntale los esfuerzos individuales y colectivos para su empoderamiento.

Blanca Lilia Ibarra Cadena
Comisionada Presidenta del INAI y del SNT

Mensaje

La Guía orientadora La Protección de Datos Personales en Plataformas Digitales promovida al interior de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia en coordinación con la Secretaría Ejecutiva del SNT, refleja el trabajo colaborativo que existe entre los Organismos Garantes del país que integran el SNT y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI.

La Guía fue concebida como una herramienta de facilitación dirigida a los titulares de los datos personales aportando conocimientos básicos que de manera preventiva permitan contar con las herramientas e información estratégica para proteger sus datos personales en el entorno de las plataformas digitales.

Este esfuerzo coordinado de colaboración entre los Organismos Garantes del país, se refleja en la Guía, la cual fue construida a través de diecisiete cuestionamientos planteados y resueltos por Comisionados de diversos Organismos Garantes. Entre los temas y cuestionamientos que se abordan encontramos los siguientes: ¿Qué son los datos personales y qué categorías existen?, ¿En qué consiste la identidad digital y cómo se relaciona con los filtros burbuja?, ¿Cuáles son los principios que sirven para proteger la información personal en entornos digitales?, ¿Cómo se pueden proteger los datos personales al utilizar las redes sociales?, ¿Qué derechos existen para proteger los datos personales en el entorno digital?, ¿Qué son las evaluaciones de impacto y por qué es importante que las instituciones públicas o privadas las realicen?, ¿Cuál es la legislación aplicable a la protección de datos personales en el entorno digital?

Las preguntas planteadas a lo largo de la Guía, nos permiten advertir que una significativa proporción de las actividades que hoy en día se realizan, desde el ámbito personal hasta el profesional, dependen de las TIC, por ello, el cuestionamiento al que alude la Guía, titulado ¿Qué son las tecnologías de la información y comunicación? facilita su conocimiento y alcances, lo cual permite identificar su importancia y repercusiones en materia de tratamiento de datos personales.

La tecnología ha facilitado la comunicación virtual en tiempos de pandemia; estudios han identificado que el acceso a redes sociales se ha diversificado, generando atomización en el número de plataformas utilizadas[4].

El beneficio que genera la utilización de las plataformas digitales al facilitar la comunicación y realización de diversas actividades de manera virtual; trae consigo aparejados diversos riesgos en el tratamiento de datos personales que son compartidos en línea, por lo que la pregunta de la Guía que aborda el tema de la identidad digital y su relación con los filtros burbuja, permitirá al lector conocer el papel que juegan los algoritmos en la construcción de identidades digitales, generando en consecuencia la conciencia y la necesidad de contar con mecanismos que protejan su información personal frente al desenfrenado desarrollo tecnológico.

En este orden de ideas, temas desarrollados en la Guía, como: la importancia de los Organismos Garantes en la protección de datos personales, el Aviso de Privacidad, la legislación aplicable a la protección de datos personales en el entorno digital, Evaluaciones de Impacto a la Protección de Datos, la Plataforma Nacional de Transparencia y el ejercicio de derechos ARCO; brindarán herramientas al lector que permitirán que conozca y cuente con el conocimiento y mecanismos legales necesarios para proteger su información personal, así como exigir el cumplimiento de la normativa en la materia.

Sin duda, el conocimiento del derecho a la protección de datos personales es pieza clave para prevenir y reducir el riesgo de sufrir alguna vulneración en el tratamiento de nuestros datos personales, es por ello que el impulso de herramientas como esta Guía, permitirá la difusión entre la población de este derecho y a su vez hará accesible a los actores involucrados en este tema, material valioso que permite tomar acciones para su debida atención.

4 17° Estudio sobre los Hábitos de los Usuarios de Internet en México 2021. Asociación de Internet MX. Mayo, 2021. Disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v15%20Publica.pdf

En suma, la Guía representa un insumo valioso para todos los integrantes del Sistema Nacional de Transparencia, es un referente construido por una parte de quienes lo conforman, que se suma al material editorial especializado que, no me cabe la menor duda, se continuará diseñando y elaborando desde el SNT y que se irá conformando como un acervo bibliográfico que permitirá aportar y compartir conocimientos y experiencias en materias propias como lo es en este caso, el derecho a la protección de datos personales.

Rosendoevgueni Monterrey Chepov
Comisionado del INAI

Índice

14 Introducción

16 Glosario

17 El Derecho a la Protección de Datos Personales en México

21 ¿Qué son las tecnologías de la información y comunicación?

24 ¿Qué son los datos personales?

27 ¿Qué categorías de datos personales existen?

30 Al utilizar Internet se comparte alguna información personal y en ocasiones se crea una identidad digital ¿En qué consiste la identidad digital?

33 ¿La identidad digital cómo se relaciona con los filtros burbuja?

36 ¿Cuáles son los principios que sirven para proteger la información personal en entornos digitales?

40 ¿Qué es un aviso de privacidad?

42 ¿Qué son los términos y condiciones descritos en aplicaciones móviles?

46 ¿Cómo se pueden proteger los datos personales al utilizar las redes sociales?

49 ¿Qué derechos existen para proteger los datos personales en el entorno digital?

52 ¿Qué son las evaluaciones de impacto y por qué es importante que las instituciones públicas o privadas las realicen?

55 ¿Qué es la privacidad digital y cuáles son sus características?

58 La importancia de los Organismos Garantes en la protección de datos personales

61 ¿Cuál es la legislación aplicable a la protección de datos personales en el entorno digital?

65 Plataforma Nacional de Transparencia y el ejercicio de derechos ARCOP

69 ¿Qué es el Recurso de Revisión de Protección de Datos Personales y dónde puede interponerse?

73 Referencias

Introducción

La presente guía representa la materialización de los esfuerzos al interior del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en cuanto al desarrollo y establecimiento de programas comunes de alcance nacional sobre el derecho a la protección de datos personales, por conducto de la Comisión de Protección de Datos Personales, que tiene como propósito ejecutar acciones de difusión, promoción, investigación y diagnóstico en esta materia.

La presente guía propone un conjunto de pautas que buscan orientar a las personas en la protección de su información personal mientras navegan por internet y cuando utilizan plataformas digitales.

En el mundo, cada año de manera progresiva aumenta la cantidad de usuarios de internet. De acuerdo al nuevo *Digital 2021 Global Overview Report* publicado por *We are Social y Hootsuite*, de los 129 millones de habitantes que actualmente tiene México, 115.4 millones cuentan con un dispositivo móvil conectado a internet, 100 millones de personas cuentan con perfiles activos en redes sociales y se estima que muchos de estos usuarios poseen más de un perfil por red social.

Las innovaciones tecnológicas de los últimos años han traído consigo diversas prácticas que en el entorno digital implican compartir información personal. La aparición de las tecnologías de la información y comunicación, así como el surgimiento en específico de plataformas digitales, aplicaciones móviles y redes sociales, por mencionar algunos ejemplos, en los hechos están reorganizando nuestra interacción social.

Compartir información personal de manera voluntaria o involuntaria en las plataformas digitales conlleva la creación de una identidad digital que define quiénes somos frente a los demás. De ahí la relevancia de conocer qué es, en qué consiste y quiénes garantizan el derecho a la protección de datos personales en México.

Por esta razón, el Sistema Nacional de Transparencia, a través de la Comisión de Protección de Datos Personales no solo participa en la generación de herramientas útiles para garantizar búsquedas seguras y con-

fiables dentro de las plataformas digitales, como la que se presenta, sino también resalta la importancia de los Órganos Garantes de las diversas entidades federativas, como actores principales en la garantía y promoción del derecho a la protección de datos personales.

Cinthya Denise Gómez Castañeda
Coordinadora de la Comisión de Protección de Datos Personales del SNT

Glosario

Constitución o Constitución Política: Constitución Política de los Estados Unidos Mexicanos.

Derechos ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales.

EIPD: Evaluación de Impacto en materia de Protección de Datos Personales.

Ley Federal o LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley General o LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

OG: Órganos Garantes.

Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

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

TIC: Tecnologías de la Información y Comunicación.

Titular: Persona física a quien corresponden los datos personales.

01

El Derecho a la Protección de Datos Personales en México

Colaboración de:
Luis Gustavo Parra Noriega
Comisionado del INFOEM del Edo. de México

El Derecho a la Protección de Datos Personales en México[5]

La primera referencia que tenemos sobre el Derecho de Protección de Datos Personales en México tiene sus antecedentes en la abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en 2002, la cual restringía su ámbito de aplicación considerando a la protección de los datos personales como un límite o excepción del derecho de acceso a la información.

A partir del año 2007, con la Reforma del artículo 6° Constitucional, se estableció la protección de la información referente a la vida privada y los datos personales; además, de establecer los primeros visos del principio de reserva de ley que facultó al Congreso a regular la materia en sus términos y excepciones, lo que implicó un importante avance en su reconocimiento.

Sin embargo, fue hasta la Reforma Constitucional de los artículos 16 y 73, fracción XXIX-O en 2009, cuando se reconoció expresamente por primera vez en México la protección de los datos personales como un derecho humano y por lo tanto, se extendió su alcance y observancia a todo el territorio nacional; además de haberse reconocido la figura de los particulares como responsables del tratamiento de los datos y la incorporación de los derechos ARCO, consistentes en los derechos de acceso, rectificación, cancelación y oposición; impactando con esto el ámbito de la autodeterminación informativa. Del mismo modo, esta reforma perfeccionó el principio de reserva de ley, confiriendo facultades al Congreso de la Unión para legislar de manera exclusiva sobre la materia. Es así como, a partir de esta reforma constitucional el derecho a la protección de datos personales fue reconocido ampliamente en México.

Como resultado de la reforma de 2009, en 2010 surgió la LFPDPPP que tiene como finalidad regular el tratamiento legítimo, controlado e informado de los mismos, así como garantizar la privacidad y el derecho a

5 Luis Gustavo Parra Noriega, Comisionado del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios.

la autodeterminación informativa de las personas. Ante el desequilibrio que prevalecía entre los distintos regímenes de protección, uno aplicable al sector privado y otro al sector público, fue necesario llevar a cabo la Reforma Constitucional en materia de transparencia de 2014, la cual trajo consigo una relevante transformación, tanto en el diseño institucional de los Órganos Garantes, a los que se otorgó autonomía constitucional y mayores facultades para la implementación de mecanismos de mayor efectividad; así como también fijó las bases para que se emitiera una ley general de protección de datos personales, que permitió dimensionar, en una situación sin precedentes, en toda su extensión el derecho a la protección de datos personales entre los entes públicos de los tres niveles de gobierno y la sociedad mexicana.

Finalmente, cabe señalar que la LGPDPPSO publicada en 2017, constituye la materialización de dicha reforma, la cual busca garantizar a cualquier persona su derecho a la protección de datos personales en posesión de Sujetos Obligados, posicionando a México a la par de los países con altos estándares contenidos en la legislación de la materia.

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

ANTECEDENTES

2002
LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

La protección de Datos Personales como un límite o excepción del Derecho de Acceso a la Información.

2007
REFORMA AL ARTÍCULO 6º CONSTITUCIONAL

Reguló la protección de la información referente a la vida privada y los datos personales; estableció los primeros visos del principio de reserva de ley que facultó al Congreso a regular la materia en sus términos y excepciones.

2009
REFORMAS A LOS ARTÍCULOS 16 Y 73, FR. XXIX-O CONSTITUCIONALES

En el art. 16 se reconoce por primera vez en México, la Protección de Datos Personales como un derecho humano; y en el art. 73 se le dio facultades al Congreso de la Unión para legislar sobre datos en posesión de particulares.

2010
LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES

Regula el tratamiento legítimo, controlado e informado de los datos personales, garantiza la privacidad y el derecho a la autodeterminación informativa.

2014
REFORMA CONSTITUCIONAL EN MATERIA DE TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES.

Fijó las bases para que se emitiera una ley general de protección de datos que permitió dimensionar, en una situación sin precedentes, en toda su extensión el derecho a la protección de datos personales entre los entes públicos de los tres niveles de gobierno y la sociedad mexicana.

2017
LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Garantiza a cualquier persona su derecho a la protección de datos personales en posesión de Sujetos Obligados en cualquier orden de gobierno.

02

¿Qué son las tecnologías de la información y comunicación?

Colaboración de:
Myrna Rocío Moncada Mahuem
Comisionada Presidenta del ITAIH de Hidalgo

¿Qué son las tecnologías de la información y comunicación?[6]

Son tecnologías que utilizan la informática, la microelectrónica y las telecomunicaciones para crear nuevas formas de comunicación a través de herramientas de carácter tecnológico y comunicacional, esto con el fin de facilitar la emisión, acceso y tratamiento de la información.

Esta nueva forma de procesamiento de la información logra combinar las tecnologías de la comunicación (TC) y las tecnologías de la información (TI), las primeras están compuestas por la radio, la telefonía y la televisión, las segundas se centran en la digitalización de las tecnologías de registro de contenidos. La suma de ambas al desarrollo de redes da como resultado un mayor acceso a la información, logrando que las personas puedan comunicarse sin importar la distancia, oír o ver situaciones que ocurren en otro lugar y, las más recientes, poder trabajar o realizar actividades de forma virtual.

Las TIC se pueden clasificar en tres categorías:

Redes: Son los sistemas de comunicación que conectan varios equipos y se componen básicamente de usuarios, *software y hardware*. Entre sus ventajas está el compartir recursos, intercambiar y compartir información, homogeneidad en las aplicaciones y mayor efectividad.

Terminales: Son los puntos de acceso de las personas a la información, algunos dispositivos son la computadora, el navegador de internet, los sistemas operativos para ordenadores, los *smartphones*, los televisores y las consolas de videojuego. Uno de los grandes beneficios que han permitido este tipo de TIC es el acceso a la información de forma global.

Servicios en las TIC: Este tipo de tecnologías ofrecen diferentes servicios a los consumidores entre los que se destacan el correo electrónico, la

6 Myrna Rocío Moncada Mahuem, Comisionada Presidenta del Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo.

búsqueda de información, la administración electrónica, el gobierno electrónico, aprendizaje electrónico y otros más conocidos como banca *online* y comercio electrónico.

¿CUÁLES SON LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN?

La combinación de ambas tecnologías, logran que las personas puedan comunicarse sin importar la distancia.

TECNOLOGÍAS DE LA COMUNICACIÓN:

- Radio
- Telefonía
- Televisión

TECNOLOGÍAS DE LA INFORMACIÓN:

- Digitalización de las tecnologías del registro de los contenidos.

03

¿Qué son los datos personales?

Colaboración de:
Myrna Rocío Moncada Mahuem
Comisionada Presidenta del ITAIH de Hidalgo

¿Qué son los datos personales?[7]

Los datos personales se refieren a cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 3, fr. II), por ejemplo: el nombre, los apellidos, la edad o el tipo sanguíneo; esta información permite identificar de una manera muy fácil a una persona determinada.

La información sobre la descripción física y genética también es un dato personal. Existen datos personales que se consideran más íntimos y que al divulgarse sin el consentimiento del titular se puede ocasionar alguna discriminación o ponerlo en riesgo, a este tipo de información personal se le denominan datos personales sensibles. La recolección de esta información por parte de una institución pública o privada debe ser estrictamente necesaria para cumplir únicamente con las finalidades por las cuales se obtuvo la información personal.

Los datos personales en todo momento pertenecen a su titular, aunque en ocasiones es necesario proporcionarlos a terceros para disfrutar de algún servicio de entretenimiento, educativo o de cualquier tipo de relación que se genere con el uso de las TIC.

7 Myrna Rocío Moncada Mahuem, Comisionada Presidenta del Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo.

¿QUÉ SON LOS
DATOS PERSONALES ?

Son los datos concernientes a una persona física mediante los cuales puede ser identificada e identificable.

04

¿Qué categorías de datos personales existen?

Colaboración de:
Luis Gustavo Parra Noriega
Comisionado del INFOEM del Edo. de México

¿Qué categorías de datos personales existen?[8]

Existen diversas categorías de datos personales que facilitan la clasificación y organización de este tipo de información. De manera enunciativa, más no limitativa, se consideran los siguientes tipos de datos personales:

Datos identificativos (nombre, domicilio, edad, firma, RFC, etc.).

Datos laborales (puesto, domicilio oficial, correo oficial, etc.).

Datos patrimoniales (cuentas bancarias, información crediticia, etc.).

Datos sobre procedimientos administrativos y/o jurisdiccionales.

Datos académicos (trayectoria educativa, título, número de cédula profesional, etc.).

Datos sobre la salud (estado de salud, enfermedades contraídas o en curso, etc.).

Datos biométricos (huella digital, reconocimiento de iris, etc.), entre otras.

Cabe señalar que, merecen una mención especial los datos personales sensibles ya que son datos que informan sobre los aspectos más íntimos de las personas, y cuyo mal uso puede provocar discriminaciones o poner en grave riesgo a su titular, como, por ejemplo:

- El origen racial o étnico;
- El estado de salud (pasado, presente y futuro);
- La información genética;
- La creencias religiosas, filosóficas y morales;
- La afiliación sindical;
- Las opiniones políticas;

8 Luis Gustavo Parra Noriega, Comisionado del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios.

- La preferencia sexual; entre otros.
- En ese sentido, estos datos requieren de especial protección y cuidado.

05

Al utilizar Internet se comparte alguna información personal y en ocasiones se crea una identidad digital, ¿En qué consiste la identidad digital?

Colaboración de:
Alma Cristina López de la Torre
Comisionada del IDAIP de Durango

Al utilizar Internet se comparte alguna información personal y en ocasiones se crea una identidad digital, ¿En qué consiste la identidad digital?[9]

La identidad digital o huella digital se define como el rastro que una persona deja en internet. Está compuesta por una gran cantidad de datos que proporcionamos, voluntaria o involuntariamente en la red, más allá de nuestro correo electrónico y dirección; fotos, videos, geolocalización, datos bancarios, historial de navegación o incluso nuestras preferencias como consumidor o cualquier otro dato que permita la identificación de un usuario en la red.

No se limita al uso de páginas web o redes sociales, sino que también se refiere a la transmisión de datos a través de actividades comerciales *online*, aplicaciones o servicios de mensajería instantánea; toda esa información, compone la imagen que proyectamos y que los demás tienen de nosotros: datos personales, comentarios, aficiones, gustos, noticias, amistades, compras, entre otros.

Ya sea por error, o por desconocimiento de los daños que provocan las acciones *online* que realizamos de forma recurrente, sin aplicar medidas de seguridad, podemos dejar expuesta nuestra identidad y convertirla en un objetivo vulnerable. Por ello, compartimos recomendaciones que tienen como objetivo mantener un ambiente seguro en internet y nos ayudan a prevenir los delitos como usurpación de identidad, entre otros.

7 consejos para proteger tu identidad digital.

- Actualiza el software regularmente.
- Navega solo por sitios web seguros.
- Usa conexiones Wi-Fi protegidas.
- Evita usar computadoras públicas para acceder a tu información personal.

9 Alma Cristina López de la Torre, Comisionada del Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales.

• Cambia tus contraseñas y claves de acceso con regularidad.
• Configura la privacidad de tus redes sociales.
• Sé precavido cuando navegues, revisa bien los enlaces antes de hacer clic sobre ellos.

06

¿La identidad digital cómo se relaciona con los filtros burbuja?

Colaboración de:
Laura Lizette Enríquez Rodríguez
Comisionada del INFO de la Ciudad de México

¿La identidad digital cómo se relaciona con los filtros burbuja?[10]

Retomando la definición de identidad digital, misma que se alimenta tras nuestro paso en internet, se configura una reputación (e-reputación) sobre nuestra persona, la cual se nutre de información proporcionada a mediano y largo plazo como usuarios: lo que posteamos y compartimos en redes, nuestro perfil laboral y toda nuestra información personal contenida en la red, dicen mucho sobre quiénes somos.

Es así como las identidades que vamos creando se relacionan con lo que se conoce como filtros burbuja, que son definidos por Eli Pariser (2017) como "el ecosistema personal de información que ha sido provisto por algoritmos". Es decir, que este concepto funciona como un filtrado de búsqueda, donde el contenido que consumimos en internet se ajusta a nuestras preferencias, que serán vinculadas por los algoritmos en relación con nuestras búsquedas previas.

De esta manera, gracias a los algoritmos utilizados al respecto es que, cada individuo obtiene búsquedas personalizadas, relacionadas con la identidad digital particular.

Sin embargo, puede ser que ante estos filtros haya información que quede fuera de nuestro alcance, por lo que nuestra percepción de la información buscada, la ideología construida y hasta nuestra propia identidad digital pudieran estar sesgadas por el delimitado universo de resultados arrojado por el filtro. Por lo que, en ocasiones, se ha señalado como desventaja de esta personalización una posible manipulación y publicaciones engañosas, así como la falta de libertad para acceder a una cantidad de contenido más vasta que aquel que resulte afín a nuestras búsquedas previas.

10 Laura Lizette Enríquez Rodríguez, Comisionada Ciudadana del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

El ideal sería alcanzar lo que Christopher Allen ha denominado identidad soberana (2016), es decir, el siguiente paso de la identidad digital, en la cual el titular tiene el control absoluto de su información personal y, por ende, de los resultados arrojados en la navegación de internet.

07

¿Cuáles son los principios que sirven para proteger la información personal en entornos digitales?

Colaboración de:
Samuel Montoya Álvarez
Comisionado del IZAI de Zacatecas

¿Cuáles son los principios que sirven para proteger la información personal en entornos digitales?[11]

La evolución del entorno digital ha propiciado un flujo indiscriminado de información e interacción en línea, lo que ha generado nuevos riesgos y nuevas formas de delinquir a través de los diversos canales que nos proporciona el internet.

Ante estos nuevos riesgos, surge la necesidad de implementar normas y acciones que permitan orientar y regular el uso y tratamiento de la información de carácter personal no solo en los entornos cotidianos, sino también en los digitales, tal es el caso de los principios de la protección de datos personales, los cuales se definen como un conjunto de reglas que determinan cómo han de obtenerse, tratarse y transferirse los datos de carácter personal. Estos principios son un soporte que brinda a los titulares certeza sobre el uso de su información y a través de los cuales, las instituciones públicas o privadas, mediante una obtención y un uso adecuado de los datos personales, pretenden regular su tratamiento.

De esta manera, el artículo 6 de la Ley Federal y el artículo 16 de la Ley General, establecen que los responsables deberán observar los siguientes principios:

Principio de licitud: Consiste en que los responsables deben recabar y tratar los datos personales conforme a las disposiciones establecidas por la Ley y demás normatividad aplicable. (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 7).

Principio de lealtad: La obtención de los datos personales no debe hacerse a través de medios engañosos o fraudulentos. (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 7).

11 Samuel Montoya Álvarez, Comisionado del Instituto Zacatecano de Transparencia, Acceso a la Información y Protección de Datos Personales.

Principio de finalidad: El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 12).

Principio de consentimiento: Este principio permite decidir de manera informada, libre, inequívoca y específica si el titular de los datos personales se encuentra de acuerdo con el uso y tratamiento de su información. (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 8).

Principio de calidad: Los datos personales proporcionados deben ser correctos, exactos y completos. (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 11).

Principio de información: El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad. (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 15).

Principio de proporcionalidad: Consiste en recabar únicamente los datos personales estrictamente necesarios e indispensables para la finalidad que se persigue y que justifica su tratamiento.

Principio de responsabilidad: Quienes traten datos personales deben asegurar, que se cumpla con los principios esenciales de protección de datos personales; comprometiéndose a velar siempre por su cumplimiento y a rendir cuentas en caso de algún incumplimiento. (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010, art. 14).

¿CUÁLES SON LOS PRINCIPIOS QUE SIRVEN PARA PROTEGER LA INFORMACIÓN PERSONAL EN ENTORNOS DIGITALES?

Los principios de la protección de datos personales se definen como un conjunto de reglas que determinan cómo han de obtenerse, tratarse y transferirse los datos de carácter personal.

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

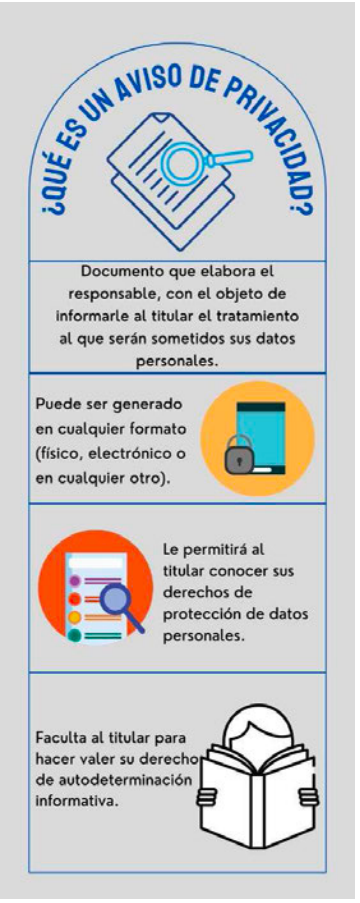
08

¿Qué es un aviso de privacidad?

Colaboración de:
Areli Yamilet Navarrete Naranjo
Comisionada Presidenta del IMAIP de Michoacán

¿Qué es un aviso de privacidad?[12]

Documento que elabora el responsable, con el objeto de informarle al titular el tratamiento al que serán sometidos sus datos personales; puede ser generado en formato físico, electrónico o en cualquier otro, y permitirá al titular conocer y ejercer sus derechos de protección de datos personales y de autodeterminación informativa.



12 Areli Yamilet Navarrete Naranjo, Comisionada del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales.

09

¿Qué son los términos y condiciones descritos en aplicaciones móviles?

Colaboración de:
Luis González Briseño
Comisionado Presidente del ICAI de Coahuila

¿Qué son los términos y condiciones descritos en aplicaciones móviles?[13]

Los términos y condiciones, o condiciones de uso y contratación, políticas de privacidad y otros documentos, son elaborados por el proveedor del servicio (en este caso de la entidad que gestiona la aplicación) y en ellos se regula la relación del usuario con respecto a los servicios que se ofrecen y los datos personales que se manejan.

La aceptación de los términos y condiciones es una de las primeras acciones que el proveedor obliga a hacer al usuario, antes de usar una aplicación, cuando se adquiere o instala.

Si bien cada proveedor redacta sus propios términos y condiciones, las legislaciones nacionales de muchos países prevén cuáles son los contenidos que un documento de este tipo debe tener.

Los términos y condiciones pueden variar enormemente según el origen de las aplicaciones o su grado de madurez y su complejidad, pero algunos contenidos típicos serían: los datos de contacto del titular, los códigos de conducta, responsabilidades y mecanismos para la resolución de conflictos, precios e impuestos, publicidad, propiedad intelectual, etc.

Dentro de la política de privacidad debe informarse de la existencia de ficheros de datos de carácter personal, de la identidad y los datos de contacto de su responsable o representante, de su finalidad y destino, y de la posibilidad de ejercer los derechos ARCO, entre otros. Por último, muchas veces se incluyen en el mismo documento, o por separado, unas reglas de uso y convivencia para los usuarios, las condiciones para los menores, e incluso el ideario de la compañía.

La importancia de los términos y condiciones no suele apreciarse cuando se está satisfecho con las aplicaciones. Sin embargo, si surge algún problema derivado de su uso que pueda acarrear pérdidas de datos o

13 Luis González Briseño, Comisionado Presidente del Instituto Coahuilense de Acceso a la Información Pública.

incluso riesgos para la privacidad del usuario o para otras personas, probablemente será cuando cobren importancia las condiciones para usar o dejar de usar el producto; así como cuáles son las responsabilidades de cada parte.

Ahora bien, ¿qué deben hacer los usuarios cuando van a instalar una nueva aplicación? Lo primero, comprobar que los documentos son accesibles, es decir, que la página abre y está en un idioma que se conoce; la segunda recomendación, hacer una lectura rápida buscando los elementos principales que se han identificado con anterioridad, o los que más causan preocupación o interés; la tercera es que, si en los términos y condiciones se percibe algo poco claro, se debe consultar a terceros o buscar otra aplicación alternativa que ofrezca más garantías; y finalmente, para el caso de las actualizaciones, el criterio de lectura puede ser el mismo: a mayor riesgo, mayor atención, y en caso de duda, considerar sustituir por otra aplicación (Agencia Española de Protección de Datos, 2018).

¿QUÉ SON LOS

TÉRMINOS Y CONDICIONES

DESCRITOS EN APLICACIONES MÓVILES?

En ellos se regula la relación del usuario con respecto a los servicios que se ofrecen y los datos personales que se manejan.

Los términos y condiciones pueden variar enormemente según el origen de las aplicaciones o su grado de madurez y su complejidad, pero algunos contenidos típicos serían, entre otros:

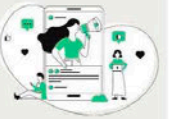
- Los datos de contacto del titular.
- Los códigos de conducta, responsabilidades y mecanismos para la resolución de conflictos.
- Los precios e impuestos.
- La publicidad.
- La propiedad intelectual.

Dentro de la política de privacidad debe informarse, entre otras cosas, de:

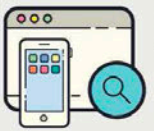
- La existencia de ficheros de datos de carácter personal.
- La identidad y los datos de contacto de su responsable o representante.
- Su finalidad y destino.
- La posibilidad de ejercer los derechos ARCO (acceso, rectificación, cancelación y oposición).

Muchas veces se incluyen en el mismo documento, o por separado:

- Reglas de uso y convivencia para los usuarios.
- Las condiciones para los menores.
- Ideario de la compañía.



¿Qué deben hacer los usuarios de aplicaciones cuando van a instalar una nueva aplicación?



1. Verificar que la página se abre y está en un idioma que se conoce.
2. Hacer una lectura rápida, buscando los elementos principales ya señalados o los que más causan preocupación o interés.
3. Al percibir algo poco claro, se debe consultar a terceros o buscar otra aplicación alternativa que ofrezca más garantías.
4. Para el caso de las actualizaciones, el criterio de lectura puede ser el mismo: a mayor riesgo, mayor atención, y en caso de duda, considerar sustituir por otra aplicación.

REFERENCIA: (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2018)

10

¿Cómo se pueden proteger los datos personales al utilizar las redes sociales?

Colaboración de:
María Elena Guadarrama Conejo
Comisionada del INFOQRO de Querétaro

¿Cómo se pueden proteger los datos personales al utilizar las redes sociales?[14]

La red social es el "conjunto de relaciones interconectadas entre un grupo de personas que ofrecen unos patrones y un refuerzo contingente para afrontar las soluciones de la vida cotidiana" (Garbarino en Quesada, 1993). A continuación, se enumeran algunas recomendaciones:

Permisos: Al usar la red social, se deben conocer los permisos que se otorgan a los proveedores del servicio, ya que es muy común que se requiera autorización para compartir contactos, fotos, micrófono entre otras cosas.

Niveles de Seguridad: Es importante configurar el nivel de seguridad lo más alto posible, con la finalidad de proteger y resguardar el contenido de personas ajenas al círculo social.

Contraseñas: Generar contraseñas seguras que no impliquen o se basen en algún otro dato personal como fecha de nacimiento, expediente laboral, teléfono celular, entre otros. Además, es recomendable actualizarlas cada tres meses.

Conexión a internet: Se debe privilegiar el uso de redes *Wi-Fi* y/o conexiones seguras (datos celulares) antes que utilizar redes abiertas o gratuitas, ya que, al conectar los dispositivos a este tipo de redes, los datos personales pueden ser más susceptibles de algún tipo de vulneración.

Geolocalización: Evitar compartir datos de geolocalización ya que se vuelve un blanco identificable una zona topográfica determinada, es recomendable mantener apagado el *GPS* y el *bluetooth* de los dispositivos.

Cierre de sesión: Fomentar el hábito de cerrar sesión cuando se entre a una red social, máxime cuando el equipo que se utiliza para ingresar no sea el propio. Hay que recordar que "cerrar" una aplicación o una ven-

14 María Elena Guadarrama Conejo, Comisionada de la Comisión de Transparencia y Acceso a la Información Pública del Estado de Querétaro.

tana del escritorio de una PC no es lo mismo que cerrar sesión, muchas veces si no se hace esto, el usuario queda expuesto a todo aquel que use el dispositivo que se utilizó.

"Amigos" desconocidos: No agregar extraños a las redes sociales. "El amigo del amigo".

Términos y condiciones de uso: Leer muy bien los términos y condiciones que solicitan las aplicaciones y/o redes sociales cuando se pueda acceder a ellas utilizando datos biométricos tales como reconocimiento facial y/o captura de huella dactilar.

11

¿Qué derechos existen para proteger los datos personales en el entorno digital?

Colaboración de:
María Antonieta Velásquez Chagoya
Comisionada Presidenta del IAIP de Oaxaca

¿Qué derechos existen para proteger los datos personales en el entorno digital?[15]

En México el derecho de protección de datos personales se encuentra previsto en distintas regulaciones, según el ámbito de que se trate. En el sector público, la Ley General regula el tratamiento de datos personales por parte de cualquier autoridad, entidad, órgano y organismo de los tres Poderes, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal, estatal y municipal. En el sector privado, la Ley Federal, cuenta con un Reglamento, Lineamientos del Aviso de Privacidad, Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del INAI, Lineamientos para el uso de hiperenlaces o hipervínculos en una página de Internet del INAI, Parámetros de Autorregulación en Materia de Protección de Datos Personales y Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante.

Además, el derecho a la protección de datos personales es un derecho humano reconocido por los artículos 6 y 16 de la Constitución Política a través de los derechos ARCO.

Acceso: Consiste en el derecho de acceder a los datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

Rectificación: Conlleva el derecho a solicitar al responsable la rectificación o corrección de los datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

Cancelación: Radica en el derecho a solicitar la cancelación de los datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por éste.

Oposición: Consiste en oponerse al tratamiento de los datos personales o

15 María Antonieta Velásquez Chagoya, Comisionada Presidenta del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Estado de Oaxaca.

exigir que se cese en el mismo, cuando aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular; los datos personales sean objeto de un tratamiento automatizado, el cual produzca efectos jurídicos no deseados o afecte de manera significativa los intereses, derechos o libertades; o estén destinados a evaluar, sin intervención humana, determinados aspectos personales o analizar o predecir, en particular, el rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

12

¿Qué son las evaluaciones de impacto y por qué es importante que las instituciones públicas o privadas las realicen?

Colaboración de:
Josefina Román Vergara
Comisionada del INAI

¿Qué son las evaluaciones de impacto y por qué es importante que las instituciones públicas o privadas las realicen?[16]

La Evaluación de Impacto en materia de Protección de Datos Personales (EIPD), es el análisis mediante el cual los responsables que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, en el cual se valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

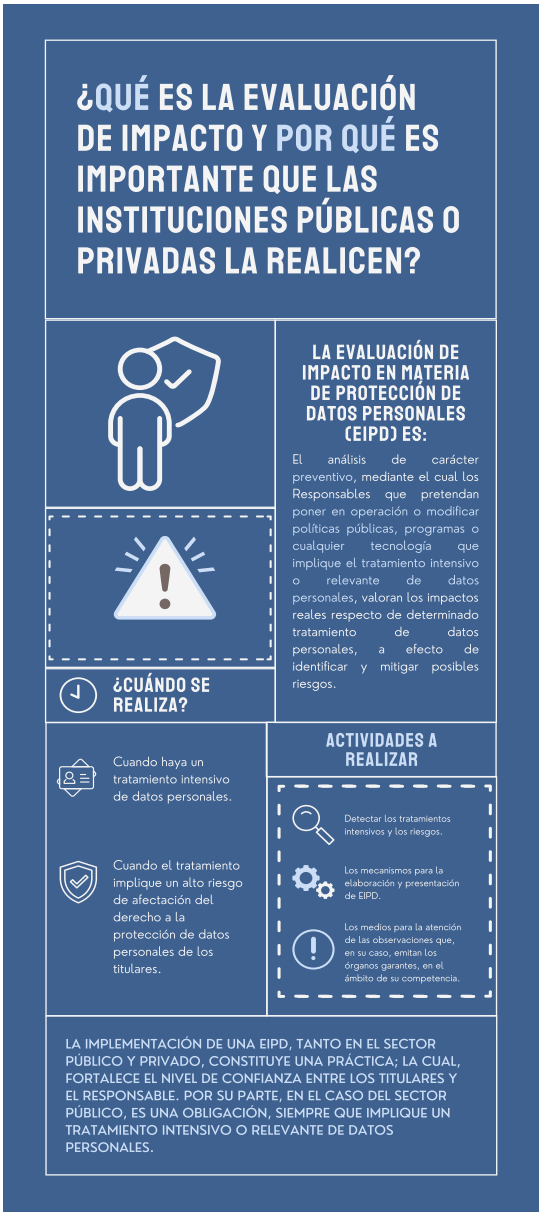
¿Cuándo se realiza un EIPD? Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, y deberá realizarse de manera previa a la implementación de éste.

Actividades a realizar: Establecer un procedimiento que prevea lo siguiente:

• Detectar los casos en que se requiera la realización de la EIPD.
• Los mecanismos para la elaboración y presentación de las Evaluaciones de Impacto en la Protección de Datos Personales.
• Los medios para la atención de las observaciones que, en su caso, emitan los OG, en el ámbito de su competencia.
• Importancia de su implementación: La implementación de una EIPD, tanto en el sector público y privado, constituye una práctica; la cual, fortalece el nivel de confianza entre los titulares y el responsable.

16 Josefina Román Vergara, Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

• Por su parte, en el caso del sector público, es una obligación, siempre que implique un tratamiento intensivo o relevante de datos personales.



13

¿Qué es la privacidad digital y cuáles son sus características?

Colaboración de:
María Teresa Treviño Fernández
Comisionada de la COTAI de Nuevo León

¿Qué es la privacidad digital y cuáles son sus características?[17]

La privacidad digital es el derecho de cualquier usuario de la red a decidir cuáles datos desea compartir, cuáles desea proteger y mantener resguardados para proteger su intimidad, pues se busca con esto, evitar que otros usuarios accedan a sus datos personales.

El concepto de privacidad digital surgió al mismo tiempo que internet y su capacidad para recopilar y compartir datos. La cantidad de información y contenidos que se pueden enviar, recibir y difundir incrementa las posibilidades de que dichos datos sean interceptados por terceros.

Características de la privacidad digital (Ley Orgánica de protección de datos personales y garantía de derechos digitales, 2018):

• Es toda la información de un usuario que circula por internet. Cuando un usuario navega en la red, deja una "huella digital" o un rastro de las acciones que ejecuta.
• Comparte ciertos datos personales como el nombre, teléfono, domicilio, datos bancarios, direcciones de correo electrónico, etc.
• Se refiere a la información que obra en imágenes, videos, geolocalización, historial de navegación, *IP* o cualquier otro dato que permita la identificación de un usuario en la red.
• Es la transmisión de datos a través de tiendas-*online*, aplicaciones, servicios de mensajería instantánea, etc.

Algunas formas de proteger la privacidad digital:

1. Configura los ajustes de privacidad en redes sociales.
2. Evita subir a la nube información personal.
3. Cambia las contraseñas de manera periódica y no uses la misma en más de un lugar.

17 María Teresa Treviño Fernández, Comisionada de la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León.

4. Mantén tu red Wi-Fi privada.
5. Lee los términos y condiciones.
6. Si realizas compras en línea, que éstas sean de preferencia ante proveedores con prestigio social, consultando experiencias de clientes anteriores.

14

La importancia de los Organismos Garantes en la protección de datos personales

Colaboración de:
Liliana Margarita Campuzano Vega
Comisionada de la CEAIP de Sinaloa

La importancia de los Organismos Garantes en la protección de datos personales[18]

Para dimensionar su relevancia y alcances en la protección de datos personales utilizados tanto en plataformas digitales como en medios físicos, hay que diferenciar que existen dos tipos de Organismos Garantes (OG) que velarán, de acuerdo con sus atribuciones y competencias por la atención, defensa, resolución de denuncias, recursos de revisión y de inconformidad, en el ejercicio de derechos ARCO.

Identificar cuál será el Organismo Garante competente para conocer sobre algún asunto, dependerá de quién es el responsable en recabar los datos para su tratamiento, es decir su manejo, uso o conservación.

En el caso de que el tratamiento de datos personales lo realicen particulares, la autoridad competente es el INAI, en términos de lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Si fue una institución pública (Sujeto Obligado) del orden estatal, es facultad de los Organismos Garantes locales; si es del orden federal, es facultad del INAI.

En la protección de datos personales y derechos ARCO, el INAI tiene atribuciones adicionales, es la segunda instancia contra resoluciones emitidas localmente y cuenta con la facultad de atracción, ya sea de oficio o a petición de los OG locales.

Además de lo anterior, el INAI y los OG locales son parte activa del SNT, trabajan en estrecha colaboración interinstitucional, para que, en el ámbito de su competencia respectiva, garantizar, promover, difundir, vigilar, verificar, capacitar, actualizar, investigar, brindar accesibilidad, publicar estudios e investigaciones, celebrar convenios, emitir lineamientos y criterios, diseñar y aplicar indicadores, divulgar estándares y mejores prác-

18 Liliana Margarita Campuzano Vega, Comisionada de la Comisión Estatal para el Acceso a la Información Pública de Sinaloa.

ticas, proporcionar apoyo a responsables y sobre todo, salvaguardar el derecho a la protección de datos personales.

15

¿Cuál es la legislación aplicable a la protección de datos personales en el entorno digital?

Colaboración de:
Arístides Rodrigo Guerrero García
Comisionado del INFO de la Ciudad de México y Secretario de la Comisión de Protección de Datos Personales de SNT

¿Cuál es la legislación aplicable a la protección de datos personales en el entorno digital?[19]

Dentro de la normatividad especializada en materia de protección de datos personales, en México tenemos la LFPDPPP del año 2010 y la LGPDPPSO del año 2016, las cuales, a pesar de haberse publicado en una época de apogeo del internet, presentan áreas de oportunidad en cuanto a los contenidos digitales.

La realidad es que en los últimos años se ha avanzado en el combate a la invasión de la privacidad de las personas usuarias de internet, sin embargo, dichos esfuerzos legislativos se encuentran fragmentados en otras normas y no en las legislaciones especializadas en materia de protección de datos personales.

Al respecto, destacan experiencias como la "Ley Olimpia", que derivó de un acto de violencia digital en el cual se compartió un video con contenido sexual sin autorización de la víctima, en el estado de Puebla. A partir de ello, la víctima y organizaciones de la sociedad civil impulsaron reformas a los Códigos Penales y leyes en al menos veintinueve entidades federativas.

A nivel federal, en noviembre de 2019 fue aprobada una reforma a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (LGAMVLV), a través de la cual se definió a la violencia digital como actos de acoso, hostigamiento, amenazas, vulneración de datos e información privada, así como la difusión de contenido sexual (ya sean fotos, videos, audios), sin el consentimiento o mediante engaños a una persona.

Asimismo, dentro de las experiencias legislativas en materia de protección de datos personales en la arena digital, destaca el reconocimiento

19 Arístides Rodrigo Guerrero García, Comisionado Ciudadano del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

del derecho de las personas trabajadoras a la desconexión digital en la Ley Federal del Trabajo, consistente en la posibilidad de abstenerse de responder comunicaciones electrónicas relacionadas con su trabajo, tales como mensajes, correos electrónicos, llamadas, entre otras, durante horarios no laborales.

Adicionalmente, el INAI en colaboración con la Secretaría de Economía han emitido los "Criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales", los cuales, resultan de utilidad para efectos del cuidado de datos personales en los servicios de cómputo en la nube.

De lo anterior se puede concluir que, si bien en México existe una regulación fragmentada y emergente de la protección de datos personales en el entorno digital, sería deseable incorporar un título específico en la LFPDPPP denominado: la protección de datos personales en el entorno digital.

LEGISLACIÓN APLICABLE A LA PROTECCIÓN DE DATOS PERSONALES

2010 Ley Federal de Protección de Datos Personales en Posesión de Particulares

2016 Ley General de Protección de Datos Personales en posesión de Sujetos Obligados

Ambas **presentan áreas de oportunidad** en cuanto a los contenidos digitales.

PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO DIGITAL SE ENCUENTRA FRAGMENTADA

En los últimos años se ha avanzado en el combate a la invasión de la privacidad de las personas usuarias de internet, sin embargo, dichos **esfuerzos legislativos se encuentran fragmentados en otras normas y no en las legislaciones especializadas** en materia de protección de datos personales

POR EJEMPLO:

LA "LEY OLIMPIA"

Derivó de un acto de violencia digital, la víctima y organizaciones de la sociedad civil impulsaron reformas a los Códigos Penales y leyes en al menos veintinueve entidades federativas.

REFORMA a la LEY GENERAL DE ACCESO DE LAS MUJERES A UNA VIDA LIBRE DE VIOLENCIA

Se definió a la violencia digital como actos de acoso, hostigamiento, amenazas, vulneración de datos e información privada, así como la difusión de contenido sexual, sin el consentimiento o mediante engaños a una persona.

LEY FEDERAL DEL TRABAJO

Destaca el reconocimiento del derecho de las personas trabajadoras a la desconexión digital que consiste en la posibilidad de abstenerse de responder comunicaciones electrónicas relacionadas con su trabajo, tales como mensajes, correos electrónicos, llamadas, entre otras, durante horarios no laborales.

El **INAI** y la **Secretaría de Economía** emitieron los **"Criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales"**, los cuales, resultan de utilidad para efectos del cuidado de datos personales en los servicios de cómputo en la nube.

16

Plataforma Nacional de Transparencia y el ejercicio de derechos ARCOP

Colaboración de:
Norma Julieta del Río Venegas
Comisionada del INAI

Plataforma Nacional de Transparencia y el ejercicio de derechos ARCOP

Las personas pueden ejercer sus derechos de distintas maneras, sin embargo, la forma más fácil de hacerlo es a través de la Plataforma Nacional de Transparencia (PNT).

¿Qué es la Plataforma Nacional de Transparencia?

Es un desarrollo informático a través del cual las personas pueden ejercer el derecho de acceso a la información pública a través de la presentación de solicitudes de información, así como el derecho a la protección de sus datos personales: Acceso, Rectificación, Cancelación, Oposición y Portabilidad (ARCOP).

¿Ante quiénes se pueden ejercer los derechos en la PNT?

Ante todas las instituciones públicas y entidades de interés público en México, incluyendo todos los niveles de gobierno, el poder legislativo, judicial, organismos autónomos, fideicomisos públicos y toda aquella persona que reciba recursos provenientes del erario.

¿Qué requisitos necesito para ejercer mi protección de datos personales en la PNT?

• Acreditar que eres el propietario de los datos personales.

• Tener una cuenta de correo electrónico o perfil en redes sociales digitales.

• Contar con acceso a internet.

¿Cómo puedo ejercer mis derechos ARCOP en la PNT?

Para poner en práctica la protección de tus datos personales en la PNT sigue los siguientes pasos:

1. Ingresa a la página web de la Plataforma: https://www.plataformadetransparencia.org.mx/

2. Dirígete a la pestaña de solicitudes de información.

3. Para realizar el proceso debes de tener una cuenta de usuario, si no la tienes sólo necesitas un correo electrónico o un perfil en redes sociales y una contraseña.

4. Una vez autentificado, deberás ingresar a la sección de solicitudes de información.

5. Posteriormente en este apartado seleccionar "datos personales".

6. Aparecerá un formulario en donde debes indicar qué tipo de derecho ARCOP ejercerás.

7. Después señala si eres el titular de los datos o eres un representante.

8. Indica el nombre de la institución pública que posee los datos personales.

9. Llena un campo en donde se describa la solicitud como tal.

10. Enseguida aparecerá un formulario en el cual debes adjuntar algún documento que acredite tu personalidad.

11. Posteriormente indica si los datos corresponden a una persona menor de edad, con incapacidad, fallecida o eres el titular.

12. Aceptar el aviso de privacidad

13. Enviar la solicitud de derechos ARCOP.

Una vez presentado el ejercicio del derecho de protección a tus datos personales, el Sujeto Obligado tiene 20 días hábiles para dar respuesta a tu petición.

Recuerda que en caso de que consideres que se violó tu derecho ARCOP puedes interponer una inconformidad ante el INAI.

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

PLATAFORMA NACIONAL DE TRANSPARENCIA

¿CÓMO EJERCER LOS DERECHOS ARCOP?

DERECHOS ARCOP

Derechos de
- Acceso,
- Rectificación,
- Cancelación
- Oposición al tratamiento de datos personales,
- Portabilidad

LA SOLICITUD PUEDE PRESENTARSE

En instituciones privadas:
- A través de correo electrónico
- De manera presencial

EN INSTITUCIONES PÚBLICAS:

- De manera presencial
- A través de correo electrónico
- La Plataforma Nacional de Transparencia

https://www.plataformadetransparencia.org.mx

PROCEDIMIENTO

- Presentación de la solicitud en formatos autorizados
- Acreditar la identidad del titular y, en su caso, la de su representante, así como la personaldiad de este último
- Verifica los requisitos en nuestra página para menores de edad, en estado de interdicción o incapacidad legal, o fallecida. **www.plataformadetrasparencia.org.mx**

17

¿Qué es el Recurso de Revisión de Protección de Datos Personales y dónde puede Interponerse?

Colaboración de:
Lucía Ariana Miranda Gómez
Comisionada del ITAIPBC de Baja California

¿Qué es el Recurso de Revisión de Protección de Datos Personales y dónde puede Interponerse?

En materia de Protección de Datos Personales, es el medio de impugnación de carácter administrativo que tiene por objeto garantizar al Titular de los datos personales por sí mismo o a través de su representante la protección de los mismos, mediante la interposición de un recurso de revisión ante el Instituto o, en su caso, ante los Organismos Garantes Locales o la Unidad de Transparencia del Responsable que haya conocido de la solicitud para el ejercicio de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición, así como portabilidad), dentro de un término que no podrá exceder de los quince días contados a partir del siguiente a la fecha de la notificación de la respuesta que haya sido debidamente notificada por parte del Sujeto Obligado correspondiente.

Transcurrido el plazo previsto para dar respuesta a una solicitud para el ejercicio de los derechos ARCO sin que se haya emitido ésta, el titular o, en su caso, su representante podrán interponer el recurso de revisión dentro de los quince días siguientes al que haya vencido el plazo para emitir la respuesta correspondiente.

El recurso de revisión se fundamenta en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para atender las quejas en contra de las respuestas emitidas, por los responsables del sector público federal a las solicitudes de ejercicio de derecho ARCO o por falta de respuestas. Para el caso de los Órganos Garantes Locales, además de ser aplicable la Ley General en materia de datos multimencionada, cuentan con sus respectivas leyes locales de Protección de Datos Personales para atender dentro de su ámbito de competencia las quejas en contra de las respuestas emitidas por los responsables del sector público estatal, a las solicitudes de derecho ARCO o por falta de respuestas. Siendo éstos los Órganos Garantes Locales, únicamente competentes para conocer las solicitudes en materia de datos de las solicitudes del sector Estatal.

El procedimiento inicia con la presentación del recurso de revisión por parte del titular o su representante, ante el INAI o la Unidad de Transparencia del Responsable a quien se realizó la solicitud de ejercicio de derechos ARCO, para el sector Federal. Para el caso de las entidades federativas reitero, que el procedimiento inicia con la presentación del recurso de revisión por parte del titular o su representante, ante los Órganos Garantes Locales o la Unidad de Transparencia del Responsable que haya conocido de la solicitud, de la Entidad Federativa que corresponda, para el caso del sector Estatal.

El recurso de revisión deberá contener para su interposición la denominación del responsable, nombre completo del titular que recurre o de su representante, domicilio, fecha en que fue notificada la respuesta o bien la fecha en que fue presentada la solicitud en caso de falta de respuesta, acto que se recurre, así como los puntos petitorios o motivos de inconformidad. Recurso de revisión que en ningún caso será necesario que sea ratificado por parte del titular o su representante.

RECURSO DE REVISIÓN DE PROTECCIÓN DE

DATOS PERSONALES

INICIO:

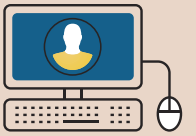
Con la presentación de un recurso de revision ante el INAI o los Organismos Garantes, según corresponda, o bien, ante la Unidad de Transparencia competente.

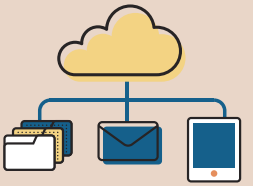
TÉRMINOS:

En un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta; o bien, transcurrido el plazo para dar respuesta sin que se haya emitido ésta, durante los 15 días siguientes al que haya vencido el plazo.

AUTORIDADES:

Se podrá interponer ante el INAI o la Unidad de Transparencia correspondiente ante quien se realizó la solicitud de ejercicio de derecho ARCO del Sector Federal; y/o ante el Órgano Garante de la Entidad o la Unidad de Transparencia correspondiente que se realizó la solicitud de derecho ARCO del Sector Estatal.





MEDIOS:

Por escrito libre al INAI, Órgano Garante de la Entidad Federativa o Unidad de Transparencia correspondiente que se realizó la solicitud ARCO, mediante correo electrónico o por formatos disponibles a través de la Plataforma Nacional de Transparencia.

REQUISITOS:

Deberá contener la denominación del responsable, nombre completo del titular que recurre o su representante, domicilio, fecha en que se fue notificada la respuesta o elaborada la solicitud, acto que se recurre, puntos petitorios o motivos de inconformidaden su caso, copia de la respuesta que se impugna y de la notificación correspondiente, y los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.

NOTA:

El Recurso de Revisión en ningún caso será necesario que sea ratificado por el titular o su representante.

Referencias

Agencia Española de Protección de Datos (2018, noviembre 29). El examen de aplicaciones (III): los términos y condiciones. ¿Por qué es importante prestar atención a los textos que acompañan a las *apps* que descargamos? [Entrada de blog]. Recuperado de: https://www.aepd.es/es/prensa-y-comunicacion/blog/el-examen-de-aplicaciones-iii-los-terminos-y-condiciones

Agencia Española de Protección de Datos (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. Recuperado de: https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Allen, Christopher (2016, abril 26). *The Path to Self-Sovereign Identity*. En *Coindesk*. Recuperado de: https://www.coindesk.com/path-self-sovereign-identity

Álvarez, Carmen (2018, marzo). Identidad digital: ¿Qué es y cómo protegerla? Regulación Financiera. En BBVA *Research*. Recuperado de: https://www.bbva.com/es/identidad-digital-protegerla/

Decreto Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno (2018, agosto 28). Diario Oficial de la Federación. En Los Estados miembros del Consejo de Europa. 28/08/2018. Recuperado de: https://www.dof.gob.mx/nota_detalle.php?codigo=5539473&fecha=28/09/2018

Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales (2018, enero 23). Diario Oficial de la Federación. En Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Recuperado de: http://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018

Gutiérrez Pérez, Macarena (2018, julio-diciembre). Ley Orgánica 3/2018 de protección de datos personales y garantías de derechos digitales. Revista La Toga, Sevilla, núm. 197, p. 94.

INAI (2019). Diccionario de Protección de Datos Personales. Conceptos fundamentales. (1ª ed.). México: Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Recuperado de: https://transparencia.guadalajara.gob.mx/sites/default/files/DiccionarioProteccionDatosPersonales.pdf

INAI (2020). Guía para la elaboración de evaluaciones de impacto a la privacidad. Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. México: Recuperado de: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/guiaeip.pdf

INAI. Guía para Titulares de los Datos Personales. Volumen 1. Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. México. Recuperado de: https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Guia%20Titulares-01_PDF.pdf

Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010, julio 5). Diario Oficial de la Federación. En Cámara de Diputados del H. Congreso de la Unión. DOF 05/07/2010. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017, enero 26). Diario Oficial de la Federación. En Cámara de Diputados del H. Congreso de la Unión. DOF. 26/01/2017. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (2018, diciembre 6). Boletín Oficial del Estado núm. 294. En Jefatura del Estado. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Lineamientos Generales de Protección de Datos Personales para el Sector Público (2018, enero 26). Diario Oficial de la Federación. En Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Recuperado de: http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

Maqueo, María Solange (Coord.). (2018). Presentación. En Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Pp. 10-13.

Pariser, Eli (2017). El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos. Editorial Taurus.

Peschard Mariscal, Jacqueline. (2013). El derecho fundamental a la protección de datos personales en México. En José Luis Piñar Mañas y Lina Ornelas Núñez Coord. La protección de Datos Personales en México. México: Tirant Lo Blanch. Pp. 19-38.

Quesada Villalba, Cristina (1993). Redes sociales: Un concepto con importantes implicaciones en la intervención comunitaria. *Psychosocial Intervention*. ISSN 1132-0559, Vol. 2, núm. 4, pp. 69-85. México. Recuperado de: http://www.copmadrid.org/webcopm/publicaciones/social/1993/vol1/arti6.htm#_Hlk421774916

Guía Orientadora "La protección de Datos Personales en plataformas digitales"

Se terminó de editar en el mes de octubre de 2021

Edición a cargo de la Secretaría Ejecutiva del Sistema Nacional de Transparencia (SNT), Dirección General de Vinculación , Coordinación y Colaboración con Entidades Federativas.