LA PRIVACIDAD EN LA ERA DE LAS REDES SOCIALES

MIGUEL RECIO GAYO

inai

Derechos Reservados D. R.
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Ciudad de México, CP 04530.
Diseño editorial: Martha Rosalba Pérez Cravioto.
Portada: Diego González Hernández.

Primera versión digital en noviembre de 2022

Hecho en México / *Made in Mexico*
Ejemplar de descarga gratuita.

Índice

Acerca del autor

Miguel Recio es doctor en derecho por la Universidad CEU San Pablo en Madrid, España. Es profesor asociado de la Facultad de Derecho de la Universidad CEU San Pablo, delegado de protección de datos y abogado del departamento de TMC de CMS Albiñana y Suárez de Lezo. Estudió la licenciatura en derecho en la Facultad de Derecho de la Universidad Carlos III de Madrid y obtuvo el máster en Protección de Datos, Transparencia y Acceso a la Información en la Universidad CEU San Pablo y un LL. M. en Derecho de la Propiedad Intelectual por The George Washington University Law School en Washington, D.C., Estados Unidos.

Abreviaturas, siglas y acrónimos

INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
Incibe	Instituto Nacional de Ciberseguridad de España
INEGI	Instituto Nacional de Estadística y Geografía
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Ontsi	Observatorio Nacional de Tecnología y Sociedad
ONU	Organización de las Naciones Unidas
Págs.	Páginas
RAE	Real Academia Española
SRS	Servicio de red social

Presentación

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) se ha propuesto implementar una política editorial que promueva entre la sociedad el conocimiento de temas con relevancia pública, y a su vez propiciar la difusión de reconocimiento sobre los dos derechos fundamentales que tutela: el acceso a la información pública y la protección de datos personales. A través de las obras editoriales, el INAI busca tender puentes y crear redes de conocimiento útiles para acercar a las instituciones públicas con la sociedad civil, y a su vez con la academia con el fin de difundir, analizar, reflexionar sobre temas que no pueden pasar desapercibidos en el actual contexto de la democracia mexicana.

El presente ensayo que usted tiene entre sus manos trata sobre las consideraciones y desafíos entorno a la agenda de la privacidad y protección de datos personales en las redes sociales digitales. El autor hace mención reiteradamente sobre las implicaciones que tiene en el ámbito legal; pero siempre poniendo en el centro la discusión sobre los usuarios de las redes sociales, lo que implica hacer efectivas las medidas necesarias para proteger la privacidad, así como el uso apropiado y proporcional de sus datos personales, los cuales, no pueden quedarse en el vacio, apelando a su vez por el uso racional y proporcional de los datos en los medios digitales.

Este texto permitirá al lector entender la figura de "privacidad" en sus múltiples ámbitos de aplicación, y explicitando cómo está prevista en la normatividad de la comunidad europea y cómo debe procesarse. Por ende, este esfuerzo editorial puede ser una buena práctica para dialogar comparativamente con otros países. A su vez, el texto permite evaluar las adecuaciones que prevén los organismos garantes en materia de protección de datos personales, y sus recomendaciones en redes digitales, las cuales, tienen como propósito lograr una interacción segura y oportuna del usuario con los espacios digitales.

Debido al aumento acelerado de los procesos de digitalización y uso de redes sociales como medio de producción, comunicación y transferencia de datos entre sociedades, instituciones y Estados, se ha vuelto imprescindible la búsqueda por asegurar/construir mecanismos que garanticen la protección de la privacidad, situación que forma parte de la discusión sobre la protección de los datos personales. Además, el autor hace referencia a una serie de circunstancias que comprometen los espacios virtuales como el grooming, ciberbullying, sexting, o manipulación masiva a través de noticias falsas, las cuales, permiten cerrar la reflexión sobre la importancia de tomar consciencia sobre el uso de las redes sociales, y lograr así una interacción adecuada y benéfica para el usuario.

Estimadas lectoras, y lectores, nuevamente el INAI a través de la presente obra, busca sumarse al dialogo imprescindible sobre la digitalización de los espacios, y la necesidad de hacer de estos un lugar seguro y útil para la ciudadanía. El texto, aunque puede ser de interés para ciertos sectores de la población como académicos y expertos en temas de datos personales, no obstante, la narrativa logra un lenguaje amigable para el público en general que desee acercarse a los temas relacionados con el establecimiento de estándares nacionales e internacionales en materia de protección de datos personales.

Comité editorial del INAI

NOTAS

1. La privacidad en la era de las redes sociales

Una de las consecuencias de la evolución de la tecnología y los servicios digitales es el cambio constante en la privacidad de las personas. Las redes sociales son un claro ejemplo de esta situación.

A principios de este siglo aparecieron las primeras redes sociales. El significado y alcance de los derechos a la protección de datos personales y a la privacidad también evolucionó de manera constante y rápida a la par de estas tecnologías.

"La privacidad en internet implica, por una parte, considerar todos los aspectos que se plantean, dada la diversidad de cuestiones que van desde el tratamiento de datos personales con fines de publicidad hasta la vigilancia electrónica, así como la interrelación que este derecho tiene con otros derechos humanos, tales como el derecho a la libertad de expresión".[1] Este principio también puede aplicarse a las redes sociales.

El uso de internet, las redes sociales y otros servicios digitales no se lleva a cabo en un vacío jurídico,[2] los usuarios deben actuar —como en cualquier otro ámbito— con precaución para evitar ser víctima de acciones ilícitas o maliciosas que pueden dar lugar al robo de datos personales o de identidad o fraudes.

Para evitar sufrir la vulneración de los derechos a la protección de datos y a la privacidad es importante conocer qué redes sociales y servicios digitales se utilizan a diario y quién las proporciona. Es

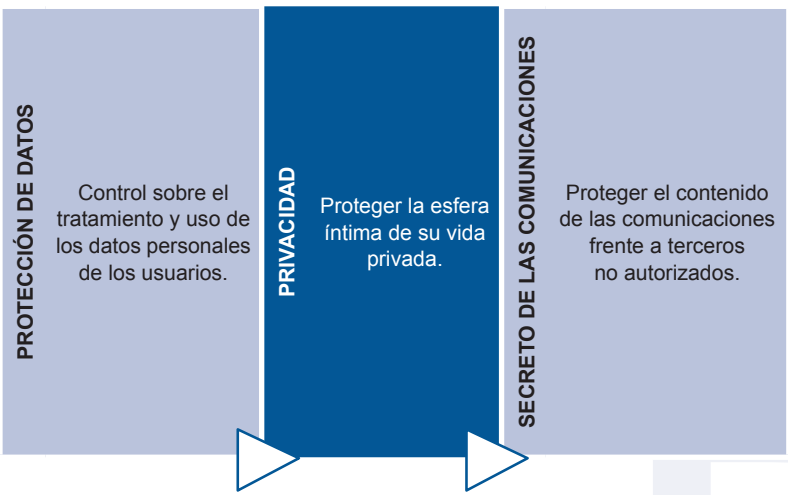
decir, debemos saber si es una empresa nacional o extranjera, qué datos personales trata, para qué los usa y qué prácticas sigue en el tratamiento de datos personales.

Es indispensable usar responsablemente las redes sociales y otros servicios digitales, evitar proporcionar más datos personales de los que son necesarios y mantenernos atentos para evitar daños u otras consecuencias que pudiera tener un uso ilícito o malicioso de nuestra información personal.

2. ¿Qué son los derechos a la protección de datos personales y a la privacidad?

Los derechos a la protección de datos personales y a la privacidad son dos derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos que respectivamente tienen por objeto proteger el derecho de las personas a controlar el uso de sus datos personales[3] y su privacidad o vida privada.[4]

A estos derechos se suma el derecho al secreto de las comunicaciones, ya que en muchos casos los usuarios de redes sociales u otros servicios digitales se comunican a través de servicios de mensajería electrónica, correo electrónico u otros servicios que se ponen a su disposición.



3. ¿Qué es una red social?

Diariamente muchas personas usan una o varias redes sociales, pero ¿qué es una red social? A continuación, veremos varias definiciones para comprender mejor qué es una red social. Puede definirse como la "estructura social formada por personas o entidades conectadas y unidas entre sí por algún tipo de relación o interés común".[5]

La Real Academia Española de la Lengua (RAE) define una red social como una "plataforma digital de comunicación global que pone en contacto a gran número de usuarios".[6] Y en el Diccionario Panhispánico del Español Jurídico se proporciona la siguiente definición de red social: "servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo".[7]

Otra definición relevante en el marco de las autoridades europeas de protección de datos que puede ser tenida en cuenta es la de servicio de red social (SRS). Por estos servicios se entienden las "plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes". [8]

Los SRS comparten las siguientes características:

- Los usuarios deben proporcionar datos personales para generar su descripción o perfil.
- Los SRS proporcionan también herramientas que permiten a los usuarios poner su propio contenido en línea (contenido generado por el usuario como fotografías, crónicas o comentarios, música, videos o enlaces hacia otros sitios).
- Las redes sociales funcionan gracias a herramientas que proporcionan una lista de contactos para cada usuario y con las que pueden interactuar.

Los SRS generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden. Los usuarios que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a las empresas que desean difundir publicidad específica y basada en esta información.[9]

Una última definición es la proporcionada por el Instituto Nacional de Tecnologías de la Comunicación en 2009 (actualmente Instituto Nacional de Ciberseguridad, Incibe), el cual define a las redes sociales como “los servicios prestados a través de internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de los usuarios afines o no al perfil publicado”.[10]

4. ¿Cómo se utilizan las redes sociales en México y quién las usa?

El uso de las redes sociales está en constante cambio. Las redes sociales aparecieron hace varias décadas, pero han evolucionado rápidamente.

En México, según las cifras proporcionadas por el Instituto Nacional de Estadística y Geografía (Inegi) en el período 2015-2020, respectivamente, se mantuvieron igual el número de usuarios de computadora que las usan como herramienta de apoyo escolar como proporción del total de usuarios de computadora y aumentó el número de usuarios de internet que han realizado transacciones (que pueden consistir en la compra de un bien, por ejemplo un libro, o la contratación de un servicio, como el alojamiento de una página web, con independencia de que se pague o no por este) vía internet como proporción del total de usuarios.

En el primer caso, el número de usuarios de computadora que las usan como herramienta de apoyo escolar, como proporción del total de usuarios de computadora, se mantuvo igual que en 2015 con un 51.3 por ciento. Este indicador sí había aumentado en 2016.

En el segundo caso, el número de usuarios que han realizado transacciones vía internet, como proporción del total de usuarios de internet, aumentó del 12.8 por ciento en 2015 al 32.7 por ciento en 2020.[11]

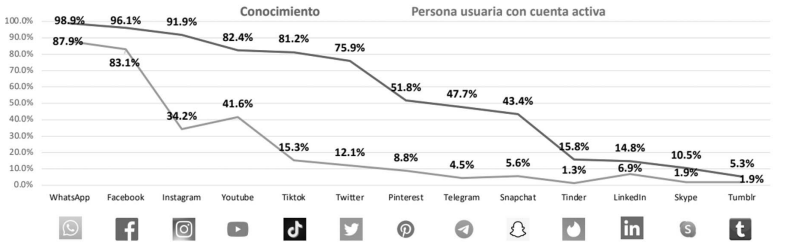
Según cifras del INAI,[12] las cinco redes sociales más utilizadas en México en 2021 fueron:

	**Facebook** Es una red social que permite la interacción entre usuarios a través de publicaciones con contenido multimedia directamente en el perfil de otro usuario o etiquetándolo en el propio perfil.
	**WhatsApp** Es una aplicación de mensajería instantánea que permite enviar mensajes y contenido multimedia a los usuarios de la misma. Actualmente, la popularidad de esta aplicación ha aumentado en México.
	**Twitter** Es una aplicación de mensajería instantánea que permite enviar mensajes y contenido multimedia. Actualmente, la popularidad de esta aplicación ha aumentado en México, es por ello que se sugiere atender recomendaciones para la protección de la privacidad.
	**YouTube** Es una aplicación para ver y compartir videos. Esta plataforma incluye una sección que permite la interacción con otros usuarios a través de comentarios en los videos y un indicador que permite señalar si el contenido les gusta o no, además de que permite denunciarlo. Es importante considerar las configuraciones de privacidad del video antes de ponerlo en la red.
	**Instagram** Esta red social permite compartir contenido multimedia a través de fotografías, videos y transmisiones en vivo con la finalidad de interactuar con otros usuarios mediante mensajes directos y comentarios en las publicaciones. Además, permite indicar si algún contenido es del agrado de los seguidores.

Fuente: Instituto Nacional de Tecnologías de la Comunicación y Agencia Española de Protección de Datos. (2019, febrero).Consultado en: https://www.uv.es/limprot/boletin9/inteco.pdf

De acuerdo con estos datos, Snapchat había descendido de las cinco primeras posiciones y YouTube se había incorporado a la cuarta posición.

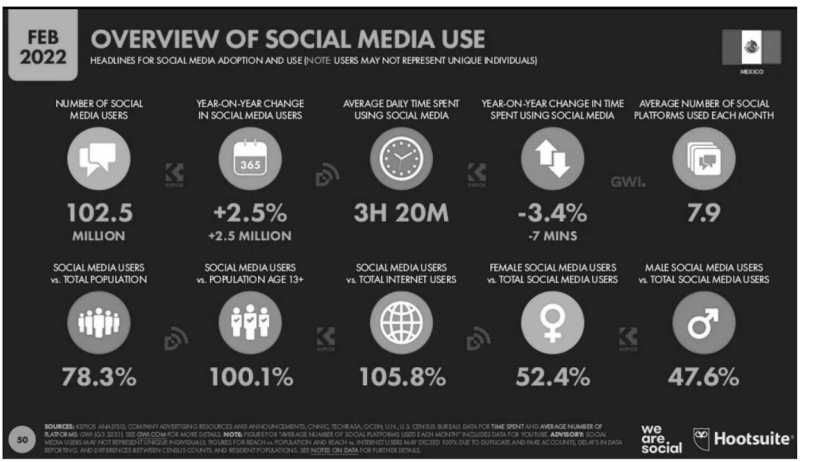
El *18º Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022*[13] indica que las redes sociales se utilizan con una frecuencia de 6.5 a la semana, en segunda posición después de la mensajería instantánea. La Asociación de Internet mx[14] señala que las cuentas activas son las siguientes:



Fuente: Asociación de Internet mx. (2022, mayo). Consultado en: https://cutt.ly/YXaNHjc

El Instituto Federal de Telecomunicaciones (IFT) ha señalado que "las redes sociales son los servicios digitales que más información recopilan de los usuarios".[15]

Según el estudio de We are social, en México, en febrero de 2022, 102.5 millones de personas hacían uso de las redes sociales, lo que representaba un 78.3 por ciento de la población mexicana activa en internet.[16] Esta cifra supone un incremento de más de 2.5 millones entre 2021 y 2022, es decir, el 2.5 por ciento.



Fuente: (DATAREPORTAL, 2022) Consultado en: https://datareportal.com/reports/digital-2022-mexico

Según el sitio Datareportal, a febrero del 2022, las redes sociales más populares entre usuarios de 16 a 64 años fueron:[17]

1. WhatsApp (94.3 %)
2. Facebook (93.4 %)
3. Facebook Messenger (80.5 %)
4. Instagram (79.1 %)
5. TikTok (70.4 %)
6. Twitter (56.0 %)
7. Pinterest (46.0 %)
8. Telegram (39.9 %)
9. Snapchat (29.8 %)
10. Skype (22.2 %)
11. Linkedin (21.6 %)
12. Discord (15.7 %)
13. Imessage (15.2 %)
14. Reddit (12.2 %)
15. Tumblr (8.4 %)

Por lo que se refiere al uso de las redes sociales en México, el INAI ofrece las siguientes cifras:[18]

REDES
sociales

Cada usuario en México

tiene en promedio **5 redes sociales**.[1]

Las principales actividades

de los usuarios de Internet en 2017, fueron: obtener información **(96.9%)**, entretenimiento **(91.4%)**, comunicación **(90.0%)**, acceso a contenidos audiovisuales **(78.1%)** y acceso a redes sociales **(76.6%)**.[2]

Facebook

es la principal red social en México.[3]

1 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid= (p.18).
2 Consultable en: http://www.beta.inegi.org.mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf
3 Consultable en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid= (p.18).

Fuente: INAI (2018) en "Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital". Consultado en: https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/5RecomendacionesPDP_Web.pdf

5. ¿Qué tipos de redes sociales existen?

Existen varios tipos de redes sociales si consideramos su enfoque.

5.1. Clasificación de redes sociales del Ontsi

Dada su relevancia a nivel internacional, en España, el Observatorio Nacional de Tecnología y Sociedad (Ontsi) distingue los siguientes tipos de redes sociales:[19]

Tipo de red social	Categorías de redes sociales por su finalidad	Clases de redes sociales
Redes sociales directas	Según la finalidad	De ocio
		De uso profesional
	Según el modo de funcionamiento	De contenidos
		Basadas en perfiles personales/profesionales
		Microblogging
	Según el grado de apertura	Públicas
		Privadas
	Según el nivel de integración	De integración vertical
		De integración horizontal
Redes sociales indirectas	Foros	
	Blogs	
Otros tipos de redes sociales	Dirigidas/no dirigidas	
	Explícitas/implícitas	

Fuente: Elaboración propia con datos del Observatorio Nacional de Tecnología y Sociedad.

Según explica el Ontsi, es importante considerar las siguientes cuestiones sobre cada uno de estos tipos de redes sociales.

5.1.1. Redes sociales directas

Las redes sociales directas son "aquellas cuyos servicios prestados a través de internet en los que existe una colaboración entre grupos de personas que comparten intereses en común y que, interactuando entre sí en igualdad de condiciones, pueden controlar la información que comparten".[20]

En este caso, los usuarios de la red crean un perfil que les sirve para relacionarse con otros y el acceso a la información disponible en el perfil dependerá de las opciones de privacidad que establezca quien ha generado o creado el perfil, por ejemplo, puede estar disponible solo para conocidos, ser privado u otras opciones.

Siguiendo la explicación del Ontsi, dentro de estas redes sociales es posible distinguir las siguientes categorías:

SEGÚN FINALIDAD Se atiende al objetivo de la persona usuaria cuando usa la red social	
De ocio	Buscan fundamentalmente entretenimiento y mejorar sus relaciones personales a través de la interacción con otras personas ya sea mediante comentarios o el intercambio de información ya sea en soporte escrito o audiovisual. Por lo tanto, se trata de potenciar las relaciones personales.
De uso profesional	En este caso, según explica el Ontsi, la persona usuaria busca "promocionarse a nivel profesional, estar al día en su campo o especialidad e incrementar su agenda de contactos profesionales".

SEGÚN EL MODO DE FUNCIONAMIENTO Se tiene en cuenta el conjunto de procesos que estructuran las redes sociales y las orientan de forma particular hacia actividades concretas	
De contenidos	El Ontsi explica que la persona usuaria "crea contenidos ya sea en soporte escrito o audiovisual que posteriormente distribuye y comparte a través de la red social con otros usuarios. Los contenidos publicados suelen estar sujetos a supervisión para comprobar la adecuación de los mismos y una vez validados pueden comentarse. Una característica interesante de este tipo de redes consiste en que la información suele estar disponible para todo usuario sin necesidad de tener un perfil creado".[21]
Basadas en perfiles personales/profesionales	Se trata de compartir el perfil personal o profesional, incluyendo información sobre la persona y su fotografía. El Ontsi indica que "en este tipo de redes suele ser obligatoria la creación de un perfil para poder ser usuario y poder emplear así todas las funciones de la red".
Microblogging	El Ontsi explica que "están diseñadas para compartir y comentar pequeños paquetes de información (que suelen medirse en caracteres), pudiendo ser emitidos desde dispositivos fijos o móviles que facilitan el seguimiento activo de los mismos por parte de sus usuarios".
SEGÚN EL GRADO DE APERTURA Se tiene en cuenta la capacidad de acceso a las mismas por cualquier persona	
Públicas	En este caso el Ontsi indica que "están abiertas a ser empleadas por cualquier tipo de usuario que cuente con un dispositivo de acceso a internet sin necesidad de pertenecer a un grupo u organización concreta".
Privadas	El Ontsi explica que estas redes "están cerradas a ser empleadas por cualquier tipo de usuario. Solo se puede acceder a ellas por la pertenencia a un grupo específico u organización privada que suele hacerse cargo del coste de la misma".

continúa

SEGÚN EL NIVEL DE INTEGRACIÓN Se tiene en cuenta el nivel de afinidad, interés e involucración en materias o actividades profesionales	
De integración vertical	"Su empleo suele estar acotado al uso por parte de un grupo de usuarios a los que aúna una misma formación, interés o pertenencia profesional".
De integración horizontal	"Su empleo no está acotado a un grupo de usuarios con intereses concretos en una materia."

Fuente: Elaboración propia con datos del Observatorio Nacional de Tecnología y Sociedad.

Como ejemplos de redes sociales directas, el Ontsi menciona a Facebook, YouTube, Wikipedia, hi5, Meetic, LinkedIn, Xing, MySpace, Fotolog, Menéame, entre otras.

5.1.2. Redes sociales indirectas

Según el Ontsi, las redes sociales indirectas son "aquellas cuyos servicios prestados a través de internet cuentan con usuarios que no suelen disponer de un perfil visible para todos existiendo un individuo o grupo que controla y dirige la información o las discusiones en torno a un tema concreto".[22] Estas redes sociales pueden ser foros o blogs.

Los foros son "servicios prestados a través de Internet concebidos, en un principio, para su empleo por parte de expertos dentro un área de conocimiento específico o como herramienta de reunión con carácter informativo. En los mismos se llevan a cabo intercambios de información, valoraciones y opiniones existiendo un cierto grado de bidireccionalidad en la medida en que puede responderse a una pregunta planteada o comentar lo expuesto por otro usuario". [23]

Los blogs son "servicios prestados a través de Internet que suelen contar con un elevado grado de actualización y donde suele existir una recopilación cronológica de uno o varios autores. Es frecuente la inclusión de enlaces en las anotaciones y suelen estar administrados por el mismo autor que los crea donde plasma aspectos que, a nivel personal, considera relevantes o de interés".[24]

5.1.3. Otros tipos de redes sociales

Otros tipos de redes sociales son las dirigidas o no dirigidas y las explícitas e implícitas.

En el caso de las redes sociales dirigidas, el usuario se limita a seguir a otras personas o contenidos. Es decir, en estas redes "la relación social no es bidireccional con lo que no es posible una interacción entre el emisor del contenido o información y el receptor de este".[25] Algunos ejemplos de redes sociales dirigidas son Twitter o una fan page en Facebook.

Las redes sociales no dirigidas son aquellas en las que sí se produce una interacción, tales como amigos en Facebook o la generación de contenidos en blogs mediante la colaboración de varias personas. En este caso "sí se establece una relación social recíproca permitiendo al receptor del contenido o información generado por el emisor, comentar u opinar sobre el mismo. Son, por lo tanto, mucho más participativas".[26]

En una red social explícita, los usuarios declaran su relación con amigos o compañeros de trabajo. Por su lado, en las redes sociales implícitas, la relación entre los usuarios se deduce por su comportamiento con personas que comparten los mismos gustos, aficiones o intereses por un tema.

5.2. Clasificación de redes sociales en función de su dimensión

Otra posible clasificación de redes sociales en función de su dimensión sería la que distingue entre:

- Redes sociales horizontales
- Redes sociales verticales
  - Por temática
  - Por actividad
  - Por contenido compartido

Las redes sociales horizontales son las que "no tienen una temática definida, están dirigidas a un público genérico, y se centran en los contactos. La motivación de los usuarios al acceder a ellas es la interrelación general, sin un propósito concreto. Su función principal es la de relacionar personas a través de las herramientas que ofrecen, y todas comparten las mismas características: crear un perfil, compartir contenidos y generar listas de contactos".[27] Algunos ejemplos de redes sociales horizontales son Facebook o Badoo.

Las redes sociales verticales se centran en temas específicos de manera que son especializadas. Estas redes sociales, según su contenido, se pueden clasificar por temática, por actividad o por contenido compartido.

Isabel Ponce, en su texto Monográfico Redes Sociales, publicado por el Ministerio de Educación del Gobierno de España en 2012, explica que de acuerdo con su temática, las redes sociales se pueden clasificar en:[28]

- **Profesionales.** Están enfocadas en los negocios y actividades comerciales. Su actividad permite compartir experiencias y relacionar grupos, empresas y usuarios interesados en la colaboración laboral. Los usuarios detallan en los perfiles su ocupación, las empresas en las que han trabajado o el currículo académico. Las más importantes son: Xing, LinkedIn y Viadeo, las cuales engloban todo tipo de profesiones, pero también existen otras específicas de un sector como HR.com que es específica para los profesionales de recursos humanos o ResearchGate, para investigadores científicos.
- **Identidad cultural.** En los últimos años, y debido al poder de la globalización, se aprecia un incremento de referencia al origen por parte de muchos grupos que crean sus propias redes para mantener su identidad. Ejemplos de esto son: Spaniards, la comunidad de españoles en el mundo y Asianave, una red social para los asiático-americanos.

- **Aficiones.** Estas redes sociales están dirigidas a los amantes de alguna actividad de ocio y tiempo libre. Encontramos redes específicas de un sinnúmero de pasatiempos, por ejemplo: Bloosee, sobre actividades y deportes en los océanos; Ravelry, para aficionados al punto y el ganchillo; Athlinks, centrada en natación y atletismo; Dogster, para apasionados de los perros o Moterus, relacionada con las actividades y el estilo de vida de motoristas y moteros.
- **Movimientos sociales.** Se desarrollan en torno a una preocupación social. Algunas son: WiserEarth, para la justicia social y la sostenibilidad; SocialVibe, conecta consumidores con organizaciones benéficas o Care2, para personas interesadas en el estilo de vida ecológico y el activismo social.
- **Viajes.** Proporcionan a los usuarios facilidades para viajar y recomendaciones para el buen desarrollo de sus travesías. Estas redes sociales les han ganado terreno a las tradicionales guías de viajes a la hora de preparar una escapada. Conectan viajeros que comparten sus experiencias por todo el mundo. Las más usadas son: WAYN, TravBuddy, Travellerspoint, Minube o Exploroo.
- **Otras temáticas.** Encontramos, por ejemplo, redes sociales especializadas en el aprendizaje de idiomas, como Busuu; plataformas para talentos artísticos, como Taltopia o sobre compras, como Shoomo.

Por actividad a la que se dedican, las redes sociales se podrían clasificar de la siguiente manera:[29]

- ***Microblogging.*** Estas redes sociales ofrecen un servicio de envío y publicación de mensajes breves de texto. También permiten seguir a otros usuarios, aunque esto no establece necesariamente una relación recíproca como los seguidores de los famosos en Twitter. Dentro de esta categoría están: Twitter, Muugoo, Plurk, Identi.ca, Tumblr, Wooxie y Metaki.

- **Juegos.** En estas plataformas se congregan usuarios para jugar y relacionarse con otras personas mediante los servicios que ofrecen. A pesar de que muchos creen que son simplemente sitios web de juegos virtuales, las redes sociales que se crean en torno a ellos establecen interacciones tan potentes que, incluso, muchos expertos de las ciencias sociales han estudiado el comportamiento de los colectivos y usuarios dentro de ellos. Algunas son: Friendster, Foursquare, Second Life, Haboo, Wipley, Nosplay y World of Warcraft.
- **Geolocalización.** También llamadas de georreferencia, estas redes sociales permiten mostrar el posicionamiento con el que se define la localización de un objeto, ya sea una persona, un monumento o un restaurante. Mediante ellas, los usuarios pueden localizar el contenido digital que comparten. Por ejemplos, Foursquare, Metaki, Ipoki y Panoramio.
- **Marcadores sociales**. La actividad principal de los usuarios de marcadores sociales es almacenar y clasificar enlaces para ser compartidos con otros y, así mismo, conocer sus listas de recursos. Estos servicios ofrecen la posibilidad de comentar y votar los contenidos de los miembros, enviar mensajes y crear grupos. Los más populares son Delicious, Digg y Diigo.
- **Compartir objetos.** Dentro de estas redes sus miembros comparten contenidos diversos como videos, fotografías o noticias, y mediante esta colaboración se establecen las relaciones que tampoco tienen que ser mutuas de forma obligatoria.

Por su contenido compartido, las redes sociales se distinguen en:[30]

- **Fotos.** Estos servicios ofrecen la posibilidad de almacenar, ordenar, buscar y compartir fotografías. Las más importantes en número de usuarios son Flickr, Fotolog, Pinterest y Panoramio.
- **Música.** Están especializadas en escuchar, clasificar y compartir música. Permiten crear listas de contactos y conocer, en tiempo real, las preferencias musicales de otros miembros. Por ejemplo, Last.fm, Blip.fm o Grooveshark.

- **Videos.** Los sitios web de almacenamiento de videos se han popularizado de tal manera que en los últimos años incorporan la creación de perfiles y listas de amigos para la participación colectiva mediante los recursos de los usuarios y sus gustos. Algunas son Youtube, Vimeo, Dailymotion, Pinterest y Flickr.
- **Documentos.** Por la red navegan documentos de todo tipo en formatos diversos, en estas redes sociales podemos encontrar, publicar y compartir los textos definidos por nuestras preferencias de una manera fácil y accesible. Su mayor exponente es Scribd.
- **Presentaciones.** Al igual que ocurre con los documentos, el trabajo colaborativo y la participación marcan estas redes sociales que ofrecen a los usuarios la posibilidad de clasificar y compartir sus presentaciones profesionales, personales o académicas. Las más conocidas son: SlideShare y Slideboom.
- **Noticias.** Existen servicios centrados en compartir noticias y actualizaciones generalmente en tiempo real que permiten al usuario ver en un único sitio la información que más le interesa y, mediante ella, relacionarse y establecer hilos de conversación con otros miembros. Algunos de ellos son Menéame, Aupatu, Digg y Friendfeed.
- **Lectura.** Estas redes sociales no sólo comparten opiniones sobre libros o lecturas, sino que además pueden clasificar sus preferencias literarias y crear una biblioteca virtual de referencias. Ejemplos de esta categoría son Anobii, Librarything, Entrelectores, weRead y Wattpad.

5.3. ¿Quién es quién en materia de datos personales en las redes sociales?

En una red social, la persona usuaria es la titular de los datos personales y el responsable de su tratamiento,[31] pero también puede haber otros actores, tales como terceros, que también son responsables o encargados del tratamiento.

Titular de los datos personales	Responsable del tratamiento
Es la persona física a quien corresponden los datos personales. En este caso es la persona usuaria de la red social.	Es la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. En este caso es la red social o un tercero que proporciona aplicaciones.

Fuente: Elaboración propia con datos del INAI. Consultado en: https://home.inai.org.mx/wpcontent/documentos/GuiasTitulares/Guia%20Titulares-01_PDF.pdf

5.3.1. El titular de los datos personales

La persona titular de los datos personales es la persona física a quien corresponden o a quien se refieren los datos personales que son tratados en relación con el uso de una red social o, incluso, en el caso de personas que no son usuarias.

Al respecto, el INAI explica que la persona titular de los datos personales es:

> La persona física a quien pertenecen y refieren los datos personales. La persona física que usa una red social es la titular de los datos personales tratados por aquélla. Por tanto, la persona titular de los datos personales es la dueña de los mismos, aunque éstos se encuentren en posesión de un tercero para su tratamiento.[32]

En relación con la persona titular de los datos personales se podría tener en consideración lo siguiente:

5.3.1.1. Niñas, niños y adolescentes

Las niñas, los niños y los adolescentes pueden ser personas usuarias de redes sociales.

Como explica José Luis Piñar Mañas "los menores y jóvenes empiezan a manejarse (y se manejan ya) con muchos mayores recursos y conocimiento que los adultos. Enfrentándose a riesgos que no siempre son capaces de identificar (como tampoco son capaces de identificarlos los adultos, no nos engañemos). Entre ellos, los riesgos que para la privacidad suponen las redes sociales en internet".[33]

Al hacer uso de las redes sociales, las niñas, los niños y los adolescentes son titulares de datos personales y tienen también otros derechos. En este sentido, las niñas, los niños y los adolescentes "requieren también una atención especial por lo que se refiere a su derecho a la privacidad en internet"[34] y también son titulares de otros derechos, reconocidos en la Ley General de Derechos de Niñas, Niños y Adolescentes, tales como el derecho a la intimidad.

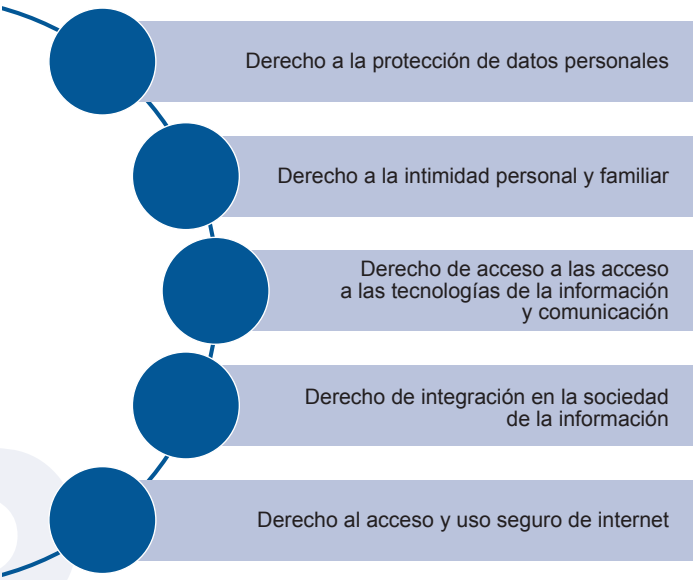
El párrafo primero del artículo 76 de la Ley General de Derechos de Niñas, Niños y Adolescentes, relativo al derecho a la intimidad, indica que "…tienen derecho a la intimidad personal y familiar, y a la protección de sus datos personales".

Otro derecho relevante que se prevé en la Ley General de Derechos de Niñas, Niños y Adolescentes es el relativo al acceso a las Tecnologías de la Información y Comunicación. En concreto, las niñas, los niños y los adolescentes "gozan del derecho de acceso universal a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido

el de banda ancha e internet establecidos en la Constitución Política de los Estados Unidos Mexicanos y en la Ley Federal de Telecomunicaciones y Radiodifusión" (artículo 101 bis). También las niñas, los niños y los adolescentes tienen derecho a la integración en la sociedad de la información, lo que incluiría el uso de los servicios de redes sociales, al indicarse que "el Estado garantizará a niñas, niños y adolescentes su integración a la sociedad de la información y el conocimiento, acorde a los fines establecidos en el artículo tercero constitucional, mediante una política de inclusión digital universal en condiciones de equidad, asequibilidad, disponibilidad, accesibilidad y calidad" (artículo 101 bis 1).

Este grupo social también "tienen derecho al acceso y uso seguro del internet como medio efectivo para ejercer los derechos a la información, comunicación, educación, salud, esparcimiento, no discriminación, entre otros, de conformidad con el principio de interdependencia, en términos de las disposiciones aplicable" (artículo 101, bis 2).

De acuerdo con el artículo 13 de la Ley General de los Derechos de Niñas, Niños y Adolescentes, estos derechos de los menores son una lista enunciativa más no limitativa. En resumen, los derechos que se reconocen a niñas, niños y adolescentes en relación o relacionados con las redes sociales son:



Fuente: Elaboración propia.

Por lo que se refiere a la protección de datos personales y la vida privada en las redes sociales e internet, cabe tener en cuenta que en 2009 se adoptó el memorándum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes, Memorándum de Montevideo.[35]

El objetivo de este memorándum es proporcionar recomendaciones que "son una contribución para que los diversos actores involucrados de la región se comprometan con el tema para extender los aspectos positivos de la sociedad de la información y conocimiento, incluyendo internet y las redes sociales digitales".

En concreto, el memorándum incluye recomendaciones dirigidas a los Estados y entidades educativas para la prevención y educación de niñas, niños y adolescentes para quienes desarrollan políticas públicas y a la industria.

5.3.2. El responsable del tratamiento

El responsable del tratamiento es la persona física o moral que decide sobre el uso de sus datos personales. En el caso de una red social o en relación con el uso de una red social, el responsable del tratamiento podría ser:

- El proveedor de la red social o proveedor de servicios de red social (SRS).
- Un proveedor de aplicaciones o *apps.*
- Otras personas morales que están en las redes sociales y que las utilizan para tratar datos personales, también denominadas socios o *partners.*

El proveedor de SRS proporciona "los medios que permiten tratar los datos de los usuarios, así como todos los servicios «básicos» vinculados a la gestión de los usuarios (por ejemplo, el registro y la supresión de cuentas). Los proveedores de SRS determinan

también la manera en que los datos de los usuarios pueden utilizarse con fines publicitarios o comerciales, incluida la publicidad proporcionada por terceros".[36]

El proveedor de aplicaciones también puede ser "responsable del tratamiento de datos, si desarrollan aplicaciones que funcionan además de los SRS y que los usuarios deciden utilizar". Por ejemplo, si hacemos uso de una aplicación que es proporcionada por otro responsable del tratamiento para su uso en lo relacionado con la red social.

Proveedor de la red social	Proveedor de aplicaciones o *apps*	Otros socios del proveedor de la red social
Proporciona el servicio de red social y otros servicios relacionados, tales como mensajería o videollamada.	Proporcionan aplicaciones que se puede hacer uso en la red social. Por ejemplo, una app de juegos, un avatar o un calendario.	Uso de los datos personales con fines de publicidad, combinación con otros datos personales o estudios y análisis de datos personales.

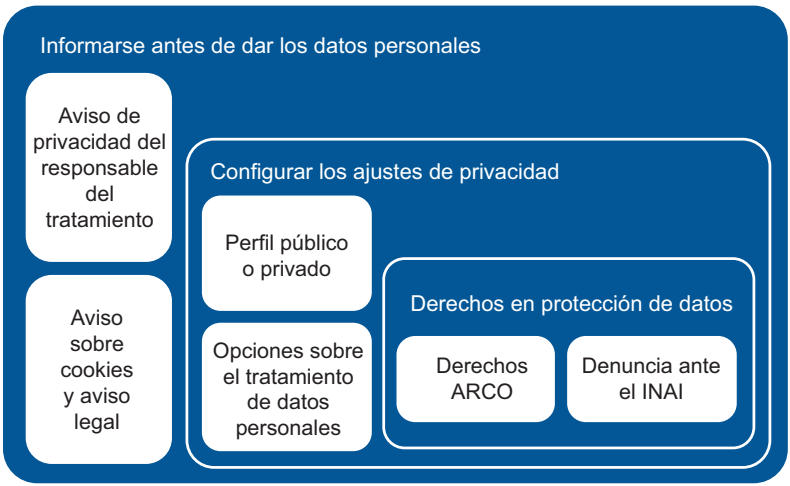
Fuente: elaboración propia.

Todos estos proveedores, tanto del servicio de red social como de aplicaciones u otros socios, son responsables del tratamiento y los usuarios de las redes sociales deben tener en cuenta lo siguiente por lo que se refiere al tratamiento de sus datos personales:

TRATAMIENTO DE DATOS PERSONALES POR LOS RESPONSABLES	RECOMENDACIONES PARA LAS PERSONAS USUARIAS DE REDES SOCIALES
☐ Cada responsable tratará los datos personales para sus propias finalidades.	☐ Leer el aviso de privacidad de cada responsable.
☐ Los responsables del tratamiento podrían transferir o comunicar los datos a otros.	☐ Ejercer los derechos ARCO.
☐ Cada responsable del tratamiento tendrá opciones de privacidad diferentes.	☐ Preguntar al responsable dudas o solicitar más información sobre el tratamiento.

Fuente: Elaboración propia.

Con la finalidad de saber quién y para qué se tratan los datos personales y poder tener el control de su uso, la persona usuaria de una red social debe considerar las siguientes recomendaciones:



Fuente: Elaboración propia con recomendaciones del INAI.

Si la persona usuaria tiene dudas sobre la configuración de los ajustes de privacidad de las redes sociales, el INAI, en sus recomendaciones para mantener segura la privacidad y datos personales en el entorno digital, incluye los pasos para configurar la privacidad de las cinco redes sociales más utilizadas en México que son Facebook, WhatsApp, Twitter, YouTube e Instagram.[37]

En el caso de las aplicaciones o *apps,* la persona usuaria de la red social debe también considerar lo siguiente:

Fuente: https://home.inai.org.mx/?page_id=6956#&gid=271c294a&pid=1

5.3.3. Terceros, socios de negocio y otros responsables del tratamiento

Los socios o *partners* son responsables del tratamiento que, por ejemplo, podrían tratar datos personales de la persona usuaria obtenidos por la red social con fines de publicidad o para combinar datos personales con los obtenidos cuando se utilizan otros servicios digitales o se proporcionan a empresas o llevan a cabo un análisis del perfil de la persona usuaria.

Es necesario leer la política de privacidad o aviso de privacidad de la red social para saber si hay terceros[38] —socios comerciales u otros— responsables del tratamiento de los datos personales recabados a través de una red social para realizar análisis o estudios de mercado.

Es decir, el tercero es otro responsable del tratamiento que recaba del interesado o recibe de la red social, como responsable del tratamiento, los datos personales para tratarlos con la finalidad que se indique en su aviso de privacidad. Es importante que cuando la persona usuaria acceda a una red social se informe sobre la existencia de estos responsables del tratamiento para saber quién trata sus datos personales y, en su caso, poder ejercer sus derechos.

5.3.4. El encargado del tratamiento

A diferencia del responsable, quien decide sobre el tratamiento de los datos personales, el encargado[39] trata los datos personales para prestar un servicio al usuario.

Por ejemplo, la persona usuaria podría acceder a la página de fans de su empresa favorita o de una persona que le ofrece contenidos de su interés en su red social. Es la red social la que, como encargada del tratamiento de esa empresa u organización, trata los datos personales de la persona usuaria para prestar el correspondiente servicio, pero no actúa como responsable del tratamiento de manera que no podría tratar los datos personales para sus propios fines, tales como enviar publicidad o realizar estadísticas.

6. ¿Qué datos personales se pueden tratar en una red social?

Dependiendo de la finalidad y uso de la red social, esta puede tratar una gran lista y variedad de datos personales de los usuarios, quienes deben ser conscientes de qué puede proporcionar y, en su caso, de que la red social puede obtener datos personales o datos personales sensibles como salud, ideología o religión. Al respecto, se debe prestar atención en la definición de ambos conceptos:

DATOS PERSONALES

Cualquier información concerniente a una persona física identificada o identificable. En este caso, la persona física es la persona usuaria de una o varias redes sociales y es titular de los datos personales.

PRIVACIDAD

Son aquellos datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos datos que puedan revelar aspectos como:

- Origen racial o étnico
- Estado de salud presente y futuro
- Información genética
- Creencias religiosas, filosóficas y morales
- Afiliación sindical
- Opiniones políticas
- Preferencia sexual

Fuente: Elaboración propia con referencia a La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

La lista de datos personales que puede tratar una red social es muy amplia y dependerá de qué uso se haga de esta, ya que una persona usuaria podría hacer un uso limitado o, por el contrario, hacer uso de varios servicios y aplicaciones ofrecidos por la red social o relacionados con esta.

A continuación, enlistamos algunos datos personales que pueden ser tratados por las redes sociales:

Ejemplos de datos personales tratados por redes sociales

- Nombre de usuario
- Contraseña
- Dirección de correo electrónico
- Número de teléfono
- Foto de perfil
- Lugar de residencia
- Lugar de nacimiento
- Fecha de nacimiento
- Edad
- Idioma(s)
- Sexo
- Estado civil
- Intereses
- Empresa u organización en la que trabaja
- CV u otros datos personales proporcionados (educación, escuela, universidad, etcétera)
- Geolocalización
- Metadatos

- Datos personales derivados del uso de la red social (desde dónde se conecta, aplicación o navegador utilizado, tiempo de conexión, páginas visitadas, etcétera)
- Si se compra algo (incluido el historial de compras) o si se hace algún pago
- Datos derivados del uso de cookies
- Amigos u otros contactos en la red social, según sea aplicable
- Grupos a los que se ha suscrito o en los que participa
- Uso de hashtags, "me gusta" o similares
- Datos proporcionados por otras personas usuarias (por ejemplo, si familiares o amigos han etiquetado a la persona usuaria en una fotografía, menciones, etcétera)
- Anuncios que vio
- Si se ha iniciado una sesión de usuario utilizando la cuenta de la red social como identificador

En su estudio *Privacidad de la Información de los Usuarios en el Uso de Servicios Digitales,*[40] el Instituto Federal de Telecomunicaciones (IFT) hace referencia a los siguientes datos personales recabados por diversas plataformas y redes sociales que operan en México:

1. Nombre
2. Correo electrónico
3. Datos de reconocimiento facial
4. Uso de servicio
5. Características del dispositivo (nivel de carga de batería, tipos y nombres de aplicaciones, cámara, etcétera)
6. Datos de pago y transacciones
7. Cookies

8. GPS
9. Registro de llamadas
10. Metadatos
11. Datos de categorías especiales (opiniones religiosas o políticas, origen étnico o racial, creencias filosóficas, etcétera)
12. Identificadores
13. Mensajes (SMS)
14. Red y conexiones
15. Historial de navegación
16. Fotos y cámara
17. Agenda de direcciones
18. Videos
19. Información de las funciones que utiliza
20. Contenido visto
21. Transacciones y métodos de pago

7. ¿Qué es el tratamiento de datos personales por una red social?

El tratamiento de datos personales consiste en la "obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales".[41] Este tratamiento de datos personales puede ser tanto en soportes físicos[42] como electrónicos,[43] siempre que sea posible el acceso conforme a criterios determinados (tales como nombre y apellidos o identificación del usuario).[44]

Como explica el INAI, "el uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia, comunicación o disposición de datos personales".[45]

Cuando las redes sociales tratan datos personales, se producen también tratamientos que son invisibles para estas. Las redes sociales pueden obtener datos personales a partir de otros datos personales, lo que se conoce también como inferir datos personales.

Cuando se infieren datos personales lo que ocurre es que el responsable del tratamiento, a partir de otros datos personales que han sido proporcionados o ha obtenido de la persona usuaria de la red social, genera nuevos datos personales.

Por ejemplo, derivado del uso que se haga de la plataforma se puede obtener cuánto tiempo ha estado conectado o conectada una persona usuaria y cuánto tiempo ha dedicado, en su caso, a ver, leer o consultar un contenido disponible en la red social de que se trate.

Además, cada vez con más frecuencia se utilizan "algoritmos para determinar qué información se muestra a qué personas"[46] en función de su perfil.

Los algoritmos utilizan datos personales para generar un modelo de algún aspecto del mundo y aplican este modelo a nuevos datos para hacer predicciones. Estos algoritmos se utilizan, por ejemplo, en el caso de la inteligencia artificial para la toma decisiones relativas a determinar qué contenido o información se muestra a unas personas usuarias de una red social y a otras.

Pero esto "puede afectar negativamente a la posibilidad de acceder a fuentes de información diversificadas en relación con un tema concreto",[47] lo que implica una desventaja o riesgo si no se hace un uso adecuado de los algoritmos y que puede ir más allá de la protección de datos personales ya que afectaría a otros derechos como la igualdad o a la información.

En el ámbito de las redes sociales otro riesgo posible, derivado de un tratamiento de datos personales que sería ilícito por vulnerar los principios de la protección de datos, en particular la finalidad del tratamiento sería "la posible manipulación de los usuarios".[48] En ese caso, quienes intentan o consiguen manipular a las personas usuarias utilizan medios de focalización o targeting "para influir en el comportamiento y las elecciones de las personas, ya sea en términos de sus decisiones de compra como consumidores o en términos de sus decisiones políticas como ciudadanos que participan en la vida cívica".[49]

Este último es otro de los riesgos a los que se exponen los usuarios de redes sociales y requiere que la persona se informe antes a través de diversas fuentes con la finalidad de evitar ser manipulada o engañada. Este riesgo ha aumentado durante la pandemia por Covid-19 y afectó directamente a los medios de comunicación, pues dio lugar a la información falsa o desinformación.

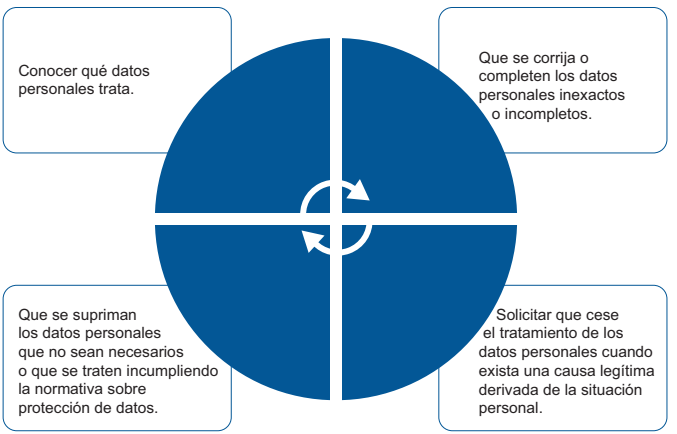
Cuestiones tales como la manipulación de las personas con información falsa durante los procesos electorales implican que la

persona usuaria de una red social u otros medios de comunicación disponibles a través de internet tengan que actuar con cuidado con la finalidad de evitar ser víctimas de acciones maliciosas o ciberdelitos u otros delitos cometidos por medios electrónicos.

8. Derechos en protección de datos

Los usuarios de redes sociales tienen derechos cuando se tratan sus datos personales, pero es necesario ver a qué legislación está sujeta la red social o el servicio digital, porque los derechos y su alcance pueden variar dependiendo de cada caso, incluso, si la red social o el servicio digital se proporcionan desde otro país. En muchas ocasiones los derechos básicos en materia de protección de datos son atendidos a través de procedimientos tales como la solicitud de borrado o eliminación de una fotografía o de un video.

Los derechos básicos ante el responsable del tratamiento en materia de protección de datos son los siguientes:



Fuente: Elaboración propia con referencia a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

9. Ventajas y desventajas de las redes sociales

9.1. Ventajas de las redes sociales

Según Luis Gustavo Parra Noriega,[50] algunas ventajas de las redes sociales pueden ser:

VENTAJAS DE LAS REDES SOCIALES

1. Se forjan nuevas conexiones personales.
2. Puede construir una identidad o personalidad en línea.
3. Se pueden conocer acciones, pensamientos y sentimientos de otras personas.
4. Se contacta con personas con los mismos intereses.
5. Se forjan nuevas amistades.
6. Se socializa y facilita la comunicación con amistades actuales.
7. Se renuevan lazos con amistades del pasado.
8. Se promueven las relaciones laborales.
9. Favorecen el trabajo colaborativo.
10. Se maximizan los negocios.
11. Diluyen fronteras o la lejanía física.
12. Facilitan las relaciones sin interés de lucro.
13. Facilitan el intercambio de información y conocimiento.
14. La comunicación puede ser en tiempo real.
15. Permiten tener información de primera mano.
16. Posibilitan una actualización más veloz comparadas con los medios tradicionales.
17. Favorecen la colaboración ciudadana.

Otras posibles ventajas de las redes sociales son:[51]

- Comunicación entre amigos.
- Comunicación entre personas que están lejos.
- Comunicación gratuita o a un coste muy reducido.
- Inmediatez en la comunicación.

- Compartir fotos, videos, etcétera.
- Sencillez de uso.
- Ahorro de tiempo y conocer personas nuevas.
- Pertenencia a grupos.
- Organización de eventos y encuentros.
- Posibilidad de expresarte de una manera más abierta.

Las redes sociales también pueden ser un medio de comunicación importante en el caso de desastres naturales. La posibilidad de enviar un mensaje a múltiples destinatarios, ya sean contactos como familiares o amigos o a cualquier persona, puede ser útil para ayudar en momentos en los que la persona usuaria no tiene otra forma de comunicación.

9.2. Desventajas de las redes sociales

Algunas desventajas de las redes sociales podrían ser:

DESVENTAJAS DE LAS REDES SOCIALES

1. Pérdida de la privacidad.
2. La información personal queda expuesta.
3. No es libre de equivocarse.
4. Las intenciones personales pueden ser malentendidas.
5. Pueden criticar sin entenderlo.
6. Pueden ofender, extorsionar, hacer *bullying*, acosar o difamar al usuario.
7. Puede haber sustracción de datos personales con fines ajenos.
8. Puede haber robos y venta de datos importantes.
9. Pueden suplantar y/o robar identidad.
10. Facilita la ubicación de su persona (física, mental y emocionalmente).
11. Facilita la ubicación de los bienes de la persona usuaria (propiedades, afectos, familia o prestigio).
12. Proveen de medios para la comisión o inducir a su comisión de delitos como pornografía, pornografía infantil y trata de personas.
13. Se suele aceptar información sin verificar.
14. Falta de análisis y selección de información.
15. Provoca distracción, pérdida de tiempo y hasta adicción.
16. Se pierden habilidades para la interacción presencial.
17. Puede desarrollar aislamiento, desvinculación y depresión.

La Agencia Española de Protección de Datos y el Instituto Nacional de Tecnologías de la Comunicación (Inteco) sugieren estas otras desventajas o posibles situaciones de riesgo para la protección de los datos personales en redes sociales:[52]

- **Casos de *phishing* y *pharming*.** Ambos fenómenos son muy explotados por los ciberdelincuentes para lograr la obtención de datos personales de los usuarios de internet, así como de datos de carácter sensible o relativos a aspectos económicos o datos de tarjetas de crédito, PIN de los usuarios, etcétera.
- **Social *spammer* y *spam*.** Es el uso de las redes sociales como plataformas para el envío de correos electrónicos no deseados.
- **Indexación no autorizada.** Se lleva a cabo por parte de buscadores de internet.
- **Acceso al perfil incontrolado.** La mayoría de las redes sociales analizadas disponen del perfil completo en formato público del usuario, o al menos de parte de este, de forma que cualquier usuario puede acceder a información de carácter personal ajena sin que el propietario de los datos tenga que dar su consentimiento expreso.
- **Suplantación de identidad.** Cada vez es más frecuente que usuarios que nunca se habían registrado en redes sociales comprueben en el momento en el que intentan acceder que su identidad digital ya estaba siendo utilizada.
- **Publicidad hipercontextualizada.** Esta aporta, a priori, una ventaja para los usuarios, ya que con ella evitan que se muestren durante su navegación contenidos irrelevantes e incluso ofensivos. Sin embargo, desde el punto de vista legal podría considerarse una práctica ilegal, ya que para poder contextualizar la publicidad que se va a mostrar a un usuario se tienen que examinar sus datos y preferencias.
- **La instalación y uso de *cookies* sin conocimiento del usuario.** Otro posible riesgo relacionado con la participación del usuario en la red social radica en la posibilidad de que el

sitio web utilice *cookies* que permitan a la plataforma conocer cuál es la actividad del usuario dentro de la misma. Mediante estas herramientas, las redes sociales pueden conocer el lugar desde el que el usuario accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de clic realizados e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la red.

La manipulación de los usuarios, la desinformación y las noticias falsas o *fake news* son desventajas y riesgos que trae consigo el uso inadecuado de las redes sociales.

Algunas posibles recomendaciones dirigidas a las personas usuarias para evitar y minimizar los riesgos derivados de acciones maliciosas como la manipulación masiva o las noticias falsas son:

Manipulación Masiva	Desinformación o Noticias Falsas
Pensar bien que tipo de información personal (intereses o datos sensibles) va a compartir en una red social, ya sea con familiares, amigos o de manera pública.	Antes de compartir, publicar, reenviar o dar clic a una "información" es importante comprobar su veracidad.

Fuente: Elaboración propia con datos de INTECO y la Agencia Española de Protección de Datos Personales.

El objetivo de estas recomendaciones es también que la persona usuaria de una red social u otros servicios digitales disponibles en internet sea responsable sobre quién, cómo y para qué se van a tratar sus datos personales y cómo utilizar de manera segura las redes sociales.

El Sistema Nacional de Protección de Niñas, Niños y Adolescentes ofrece algunas recomendaciones para evitar riesgos en las redes sociales. Estas recomendaciones son las siguientes:

	**1. Ningúna Información en línea es privada** Un “amigo” puede difundirla y dispensarla en cualquier momento.
	**2. Regla de Oro** Los controles automáticos digitales jamás deben reemplazar la supervisión parental en vivo.
	**3. Algunos Riesgos** Pueden recibir mensajes de un extraño malintencionado y encontrarse físicamente con un desconocido o ser acosados por sus semejantes, pues no hay manera de verificar la edad de la persona con la que se comunican, pueden ver videos o foros provocativos que les causen daño, les dan acceso a grupos no aptos para su edad y desarrollo.
	**4. Algunas Reglas** Dialogue y mantenga abierta la comunicación cpn sus hijas e hijos. Tenga interés por sus actividades y amistades digitales; ponga atención en la información que comparte en redes (fotos y videos). Enséñeles como pueden proteger la información propia y a respetar la de los demás, averigüe y enseñe como protegerse de los ciberacosadores, cheque que usen los controles de privacidad de las redes, insista en que eviten encontrarse con alguien que sólo conoce por internet.
	**5. Algunas Herramientas** Ponga los filtros de edades, use programas para monitorear, en especial si sospecha que sus hijas e hijos peligran en la red, revise el historial en internet, sea cuidadoso con los chats que usanm en especial en vivo, use buscadores seguros y controles de padres en teléfonos y otros *gadgets*.

Fuente: Elaboración propia con información del Sistema Nacional de Protección de Niñas, Niños y Adolescentes.

En materia de protección de datos personales en las redes sociales, el INAI ofrece también las siguientes recomendaciones:

Fuente: (INAI, 2019) " 7 recomendaciones de seguridad para proteger tus datos personales". Consultado:https://m.facebook.com/INAImx/posts/-conoce-las-7-recomendaciones-de-seguridad-para-proteger-tus-datospersonales-en-/2451374014917074/

En España, el INTECO y la Agencia Española de Protección de Datos (2009) publicaron una serie de recomendaciones para hacer un uso seguro de las redes sociales:

> Con la intención de que puedan conocer todos y cada uno de los beneficios que este tipo de servicios online pueden aportar a sus vidas, pero sin descuidar el conocimiento sobre la existencia de determinadas situaciones desfavorables, que sin embargo pueden ser fácilmente evitables.

Estas propuestas se estructuran atendiendo a la protección de datos personales, honor, intimidad y propia imagen, a la propiedad

intelectual, recomendaciones de carácter tecnológico y de seguridad y a la protección de los menores.

1. Se recomienda a todos los usuarios recurrir al uso de seudónimos o *nicks* personales con los que operar a través de Internet, permitiéndoles disponer de una auténtica "identidad digital", que no ponga en entredicho la seguridad de su vida personal y profesional. De esta forma, únicamente será conocido por su círculo de contactos, que conocen el *nick* que emplea en Internet.
2. Se recomienda a los usuarios tener especial cuidado a la hora de publicar contenidos audiovisuales y gráficos en sus perfiles, dado que en este caso pueden estar poniendo en riesgo la privacidad e intimidad de personas de su entorno.
3. Se recomienda revisar y leer, tanto en el momento previo al registro de usuario, como posteriormente, las condiciones generales de uso y la política de privacidad que la plataforma pone a su disposición en sus sitios web.
4. Se recomienda configurar adecuadamente el grado de privacidad del perfil de usuario en la red social, de tal forma que éste no sea completamente público, sino que únicamente tengan acceso a la información publicada en el perfil aquellas personas que hayan sido catalogadas como "amigos" o "contactos directos" previamente por el usuario.
5. Se recomienda aceptar como contacto únicamente a aquellas personas conocidas o con las que mantiene alguna relación previa, no aceptando de forma compulsiva todas las solicitudes de contacto que recibe e investigando siempre que fuera posible y necesario, quién es la persona que solicita su contacto a través de la red social.
6. Se recomienda no publicar en el perfil de usuario información de contacto físico, que permita a cualquier persona conocer dónde vive, dónde trabaja o estudia diariamente o los lugares de ocio que suele frecuentar.

7. A los usuarios de herramientas de *microblogging* se recomienda tener especial cuidado respecto a la publicación de información relativa a los lugares en que se encuentra en todo momento.
8. Se recomienda utilizar y publicar únicamente contenidos respecto a los que se cuente con los derechos de propiedad intelectual suficientes. En caso contrario, el usuario estará cometiendo un ilícito civil protegible por parte de los tribunales nacionales.
9. Se recomienda a los usuarios emplear diferentes nombres de usuario y contraseñas para entrar en las distintas redes sociales de las que sea miembro.
10. Se recomienda utilizar contraseñas con una extensión mínima de 8 caracteres, alfanuméricos y con uso de mayúsculas y minúsculas.
11. Se recomienda a todos los usuarios disponer en sus equipos de software antivirus instalado y debidamente actualizado.
12. Los menores no deben revelar datos personales excesivos. Nunca se deben suministrar los datos a desconocidos.
13. Se debe leer toda la información concerniente a la página web. En ella se explica quiénes son los titulares de esta y la finalidad para la que se solicitan los datos.
14. Si el usuario es menor de catorce años, se necesita también el consentimiento de los padres o tutores. En estos casos, siempre que se soliciten datos por parte de una red social debe preguntarse a los padres o tutores para ver si ellos aprueban la suscripción o no.
15. No deben comunicarse a terceros los nombres de usuario y contraseña, ni compartirlos entre amigos o compañeros de clase. Estos datos son privados y no deben ser comunicados a terceros y/o desconocidos.
16. Siempre que se tenga cualquier duda respecto a alguna situación que se derive del uso de las redes sociales y herramientas

colaborativas, debe preguntarse a los padres o tutores.

17. Se debe mantener el ordenador en una zona común de la casa.
18. Se deben establecer reglas sobre el uso de Internet en casa.
19. Los padres deben conocer el funcionamiento y las posibilidades de este tipo de plataformas, tanto positivas como negativas.
20. Activar el control parental y las herramientas de control de la plataforma, así como establecer el correo del padre o tutor como correo de contacto secundario.
21. Asegurarse de que los controles de verificación de la edad están implementados.
22. Asegurar la correcta instalación del bloqueador de contenidos.
23. Concienciar e informar a los menores sobre aspectos relativos a la seguridad.
24. Explicar a los menores que nunca han de quedar con personas que hayan conocido en el mundo online y que si lo hacen debe ser siempre en compañía de sus padres o tutores.
25. Asegurarse de que los menores conocen los riesgos e implicaciones de alojar contenidos como videos y fotografías, así como el uso de cámaras web a través de las redes sociales.
26. Controlar el perfil de usuario del menor.
27. Asegurarse de que el menor sólo accede a las páginas recomendadas para su edad.
28. Asegurarse de que los menores no utilizan su nombre completo.[53]

Inteco y la Agencia Española de Protección de Datos también hacen recomendaciones específicas en materia de tecnología y seguridad, así como protección de niñas, niños y menores:[54]

Tecnológicas y de seguridad

- **Se recomienda a los usuarios emplear diferentes nombres de usuario y contraseñas para entrar en las distintas redes sociales** de las que sea miembro. Esta medida procura aumentar el grado de seguridad del perfil de usuario, dado que los posibles atacantes no deberán romper la seguridad de un único sistema de acceso.
- **Se recomienda utilizar contraseñas con una extensión mínima de 8 caracteres, alfanuméricos y con uso de mayúsculas y minúsculas.** Este tipo de contraseñas certifica que el grado de seguridad del acceso es elevado, garantizando de esta forma una mayor integridad de la información publicada.
- **Se recomienda a todos los usuarios disponer en sus equipos de software antivirus instalado y debidamente actualizado,** que garantice que su equipo se encuentra libre de software maligno, así como de aplicaciones spyware que pongan en riesgo su navegación en Internet, y en peligro la información alojada en el equipo.

Protección de menores

- **No se deben revelar datos personales excesivos.** Hay personas que quieren aprovecharse de los datos de los menores para acceder a un grupo de usuarios o simplemente para recolectar perfiles. Nunca se deben suministrar los datos a desconocidos. En caso de duda, lo más recomendable es preguntar a los padres o tutores.
- **Se debe leer toda la información concerniente a la página web.** En ella se explica quiénes son los titulares de la misma y la finalidad para la que se solicitan los datos.
- **Si el usuario es menor de catorce años, se necesita también el consentimiento de los padres o tutores.** En estos casos, siempre que se soliciten datos por parte de una red social debe preguntarse a los padres o tutores para ver si ellos aprueban la suscripción o no.

- **No deben comunicarse a terceros los nombres de usuario y contraseña, ni compartirlos entre amigos o compañeros de clase.** Estos datos son privados y no deben ser comunicados a terceros y/o desconocidos.
- **Siempre que se tenga cualquier duda respecto a alguna situación que se derive del uso de las redes sociales y herramientas colaborativas, debe preguntarse a los padres o tutores.** En caso de detectar una conducta no agradable por parte de otro usuario, lo mejor es comunicárselo a los padres o tutores y denunciar a ese usuario dentro de la propia plataforma, para que se tomen las medidas oportunas con respecto a éste a través de los medios internos con los que las propias plataformas cuentan.

  En caso de considerar tal conducta como delictiva, se debe comunicar también a las Fuerzas y Cuerpos de Seguridad del Estado, que cuentan con brigadas especializadas en este tipo de situaciones.

Respecto a las **recomendaciones especialmente dirigidas a los padres o tutores,** se establece que:

- **Se debe mantener el ordenador en una zona común de la casa,** sobre todo cuando los menores utilicen Internet. En su defecto, se recomienda utilizar herramientas de monitorización que permitan conocer las rutas de navegación de los menores y que éstos no puedan eliminar ni desbloquear dichos contenidos.
- **Se deben establecer reglas sobre el uso de Internet en casa.** En el momento en que los menores empiecen a utilizar Internet de forma independiente, se deben establecer reglas respecto al tipo de contenidos que pueden visitar, incluidas las redes sociales, así como las horas al día de utilización de las mismas.
- **Los padres deben conocer el funcionamiento y las posibilidades de este tipo de plataformas, tanto positivas como negativas.** Así, se podrán conocer las posibles implicaciones jurídicas y tecnológicas que pueden derivarse de su uso, y de otro lado, educar en su utilización de una forma más experta.

- **Activar el control parental y las herramientas de control de la plataforma, así como establecer el correo del padre o tutor como correo de contacto secundario.** Además, de esta manera, cualquier anuncio o petición proveniente de la plataforma llegará a la dirección del correo electrónico del padre o tutor, pudiendo éste conocer las actividades que realiza su hijo. Con este sistema, para la incorporación a ciertos grupos será necesaria la autorización de los padres o tutores.
- **Asegurarse de que los controles de verificación de la edad están implementados.** Asegurarse de que las páginas a las que acceden los menores disponen de sistemas de reconocimiento de edad, así como de información previa respecto al tipo de contenidos mostrados en el sitio web.
- **Asegurar la correcta instalación del bloqueador de contenidos.** El uso de este tipo de herramientas puede prevenir el acceso a contenidos no recomendables para menores, tanto desde el ordenador, como desde dispositivos móviles. Con esta herramienta, todo contenido para mayores de edad o sin clasificación de edad será bloqueado.
- **Concienciar e informar a los menores sobre aspectos relativos a la seguridad.** La educación es crucial. Hay que explicar a los menores los principios básicos para llevar a cabo una navegación segura en el entorno de estas plataformas.
- **Explicar a los menores que nunca han de quedar con personas que hayan conocido en el mundo online y que si lo hacen debe ser siempre en compañía de sus padres o tutores.** Se debe evitar que los menores acudan a citas presenciales con personas que no conocen personalmente y respecto a las que sólo cuentan con un contacto online, los padres o tutores deberán acompañarlos.
- **Asegurarse de que los menores conocen los riesgos e implicaciones de alojar contenidos como videos y fotografías, así como el uso de cámaras web a través de las**

redes sociales. Es necesario explicar a los menores que el uso de fotografías y videos puede suponer un riesgo. Por ello es necesario enseñarles cómo y cuándo utilizar este tipo de herramientas.

- **Controlar el perfil de usuario del menor.** Es recomendable revisar el tipo de información que el menor está utilizando y qué tipo de datos pone a disposición del público y del resto de usuarios de la red social. Además, se recomienda realizar una revisión de las condiciones aplicadas respecto de su privacidad.
- **Asegurarse de que el menor sólo accede a las páginas recomendadas para su edad.** Así se asegurará que el resto de usuarios de la red tienen una edad semejante a la del menor, manejándose en un entorno en el que se sentirá cómodo y en el que los riesgos son menores. En caso de no conseguir encontrar la edad recomendada, la mejor solución es preguntar a la propia red social o, en su caso, bloquear el contenido.
- **Asegurarse de que los menores no utilizan su nombre completo.** De esta forma serán más difícilmente identificables por terceros malintencionados. Además, se debe potenciar el uso de pseudónimos dentro de las propias plataformas."[55] (adaptadas):

Y autoridades de protección de datos en otros países, por ejemplo, la Agencia Española de Protección de Datos, el Instituto Nacional de Ciberseguridad (INCIBE) y la Oficina de Seguridad del Internauta (OSI) hacen énfasis en una serie de recomendaciones que van encaminadas en un mismo sentido:

- **Pensar antes de publicar información en la red social.** Debe ser consciente de que la información que comparte en una red social puede ser vista por terceras personas sin su conocimiento. Esto se debe a que las personas a las que da acceso a su información eligen a su vez quien puede tener acceso a su perfil: amigos, amigos de amigos o todo el mundo. Por tanto, aunque parezca que tiene controlado con quien

comparte aspectos privados de su vida, siempre puede haber una pérdida de control de la información: si comparte una foto con sus contactos, y uno de ellos da un "Me gusta", un amigo de su contacto, al cual usted no conoce, ¿podrá ver esa foto? Antes de publicar información personal en una red social, piense qué quiere compartir y con quién.

- **¡No publique más información de la necesaria!** Cuando se registre, algunas redes sociales le solicitarán muchos datos: domicilio, lugar de trabajo, colegio, gustos, aficiones, familiares, etc., que no son obligatorios. **Valore qué información personal quiere proporcionar.**

Hay cierto tipo de **información que no debería publicar en sus perfiles** para que no comprometa su privacidad ni sea utilizada en su contra dando lugar a problemas o conflictos personales o laborales:

- Datos personales
- Contraseñas
- Datos bancarios
- Teléfono móvil
- Planes para las vacaciones
- Comportamientos inapropiados
- Insultos, palabras malsonantes
- Ideologías
- Datos médicos o relativos a su salud

Su perfil en una red social no debería ser una puerta abierta a su intimidad personal.

Además, con el paso de los años, lo que publica en Internet se convierte en su **reputación digital.** Empresas, compañeros de trabajo, amigos, etc. pueden tener una imagen suya condicionada a la información personal publicada en la Red.

¡A su información que sólo acceda quien usted quiera! Revise las **opciones de configuración** de cada red social para tener controlados los principales aspectos de privacidad y seguridad:

- Conocer quién tiene acceso a sus publicaciones
- Saber quién le puede etiquetar
- Si su perfil está visible a los buscadores de iinternet
- Conocer la geolocalización de las publicaciones, etc.

10. Ciberseguridad

La ciberseguridad es esencial para salvaguardar nuestra identidad digital, así como para hacer transacciones electrónicas o uso de servicios digitales, entre los que se encuentran las redes sociales.

Sin ciberseguridad los derechos a la protección de datos personales, a su privacidad y al secreto de las comunicaciones no serían posibles. Es decir, la ciberseguridad protege también estos derechos y permite hacerlos efectivos.

Por ejemplo, si una persona se conecta a una red abierta sobre la que no tiene control, por ejemplo en un hotel, durante una conferencia o en el transporte público, se podría dar el caso de que sus comunicaciones y sus datos sean interceptados por un tercero malicioso ya que la información, al no haber sido cifrada, viaja sin protección. Utilizar el cifrado puede ayudar a evitar este tipo de ciberataques, donde personas no autorizadas interceptan la comunicación de terceros y roban sus datos personales.

Según American Chamber México, los problemas más comunes que enfrentan los usuarios de internet en nuestro país son:[56]

Problemática	Número de personas que sufren este problema	Porcentaje del universo total de usuarios de internet en México
Exceso de información no deseada	20.5 millones de usuarios	25.5 %

continúa

Violación a la privacidad	2.5 millones de usuarios	3.1 %
Mensajes de personas desconocidas	16.4 millones de usuarios	20.3 %
Infección por virus	10.6 millones de usuarios	13.1 %
Fraudes con información financiera o personal	3.2 millones de usuarios	4.0 %

Fuente: American Chamber (2019). Consultado en: https://cutt.ly/gXsZLwV

En el caso de los fraudes con información personal, es importante considerar el robo de identidad. Ante esta situación, el INAI recomienda:[57]

- Utilizar distintas contraseñas y nombres de usuario para diferentes sitios.
- Antes de crear una cuenta en alguna red social asegúrese de haber leído sus políticas de privacidad.
- Configurar la privacidad de las redes sociales, no aceptar cualquier solicitud de amistad a menos que se encuentre seguro de conocer de forma personal a quien se la envía.
- Pensar antes de publicar información personal.
- No compartir más información de la necesaria en redes sociales.
- Configurar los niveles de privacidad entre los contactos.

El cibercrimen es una preocupación creciente[58] en muchos países alrededor del mundo, incluido México. Por esta razón, es importante que se siga avanzando en el desarrollo de una cultura de ciberseguridad. Según el Banco Interamericano de Desarrollo en 2020, en comparación con 2016, se produjeron avances en cuestiones tales como la confianza y seguridad en internet o la comprensión de la persona usuaria en la protección de la información personal (datos personales) en línea. El siguiente gráfico muestra la evolución de estos indicadores:[59]

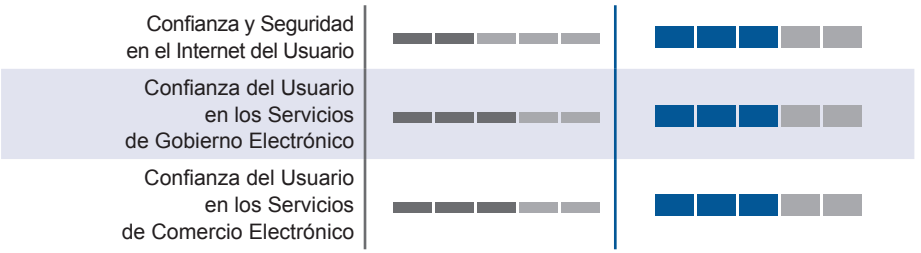
D2

2016	2020

Cultura Cibernética y Sociedad

2-1 Mentalidad de Seguridad Cibernética

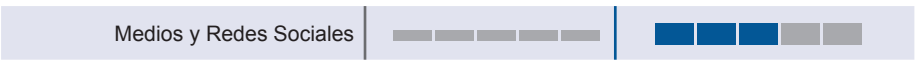
2-2 Confianza y Seguridad en Internet



2-3 Comprensión del Usuario de la Protección de la Información en Línea

2-4 Mecanismos de Denuncia

2-5 Medios y Redes Sociales



Fuente: Banco Interamericano de Desarrollo (2020). Consultado en: https://cutt.ly/tXsBXZY

Cuando se usa una red social, es necesario seguir estas recomendaciones en materia de ciberseguridad:

	**Nombre de Usuario y Contraseña** - Usar contraseñas robustas. - Utilizar un nombre de usuario y contraseñas diferentes para cada red social o servicio digital. - Cambiar la contraseña con frecuencia. - No utilizar la opcion de recordatorio de contraseña.
	**Cuidar las conexiones a la Red Social** - Comprobaar que la conexión sea segura (https). - Evitar el uso de conexiones a internet no seguras. - Cerrar la sesión cada vez que se salga de una Red Social.
	**Si se es víctima de un delito o de un tratamiento ilícito de Datos Personales** - Denunciar ante las autoridades competentes. - Denunciar ante el INAI el tratamiento ilícito de los datos personales.

Fuente: Elaboración propia con datos del INAI. Consultado en https://home.inai.org.mx/wpcontent/documentos/GuiasTitulares/Gu%C3%ADa_Prevenir_RI.pdf

El INAI ofrece las siguientes recomendaciones[60] adaptadas que pueden usarse en el caso del robo de identidad, las cuales también se pueden aplicar como buenas prácticas de navegación por internet para proteger las cuentas y dispositivos de los usuarios.

- Evitar usar computadoras públicas para acceder a la información personal, y en caso de ser necesarios, es importante limpiar el historial al terminar de navegar.
- Si se utilizan los equipos públicos para acceder a internet, se debe evitar realizar operaciones bancarias en línea.
- Si se requiere abrir una cuenta personal en una computadora de acceso público, se debe cerrar correctamente al concluir el uso del equipo.
- Si en el navegador aparece una ventana emergente que recomienda recordar contraseñas, siempre hay que indicar la opción “No”.
- Al terminar de usar el navegador, hay que borrar los datos del navegador como el historial de descargas, los datos de formularios almacenados, cookies, contraseñas y licencias de

contenido. El borrado se puede hacer accediendo a la configuración del navegador y seleccionando la opción “Borrar datos de navegación”.

- Asegurarse de cambiar las contraseñas y claves de acceso con regularidad.
- Usar contraseñas seguras y que cumplan con una serie de requisitos, por ejemplo, tener una longitud mayor a ocho distintos caracteres e incluir letras mayúsculas y minúsculas, números y símbolos.
- Proteger las computadoras, teléfonos inteligentes o tabletas con un software de seguridad o antivirus y contraseñas seguras.
- Utilizar contraseñas en todos los dispositivos que se usen y no compartirlas con terceros.
- No permitir el acceso remoto a la computadora personal.
- Proteger la información personal de los dispositivos.
- No conectarse a redes inalámbricas que no tengan contraseñas.
- Descargar aplicaciones de tiendas oficiales y de desarrolladores confiables.
- Evitar almacenar cantidades excesivas de datos personales sin cifrar en un dispositivo móvil, tales como nombres de usuario, palabras clave, información crediticia o de identificación personal, para evitar que sus datos sean interceptados si el dispositivo es extraviado.
- Antes de que se deje de utilizar, se venda o se deseche un dispositivo electrónico, se debe borrar toda la información personal y restaurar la configuración de fábrica.

Al hacer uso de redes sociales hay que actuar con precaución para evitar riesgos derivados de acciones ilícitas o maliciosas de terceros, además del robo de identidad y otras ya mencionadas.

Algunas de estas acciones maliciosas pueden ser:

Grooming

El *grooming* implica que un adulto se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual.
(Fuente: *Save the Chldren*)

Ciberbullying

El *ciberbullying* es una adaptación de las palabras en ingles *cyber* y *bullying* que en español lo conocemos como ciber abuso o violencia entre iguales.
Éste término se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente a través de internet o cualquier medio de comunicación como teléfonos móviles o tabletas.

(Fuente: gob.mxhttps://www.gob.mx/ciberbullying/artículos/que-es-el-ciberbullying)

Sexting

Consiste en el envío de forma voluntaria de imágenes o videos de contenido sexual a través de *smartphones* o dispositivos electrónicos.

(Fuente: Fundación en Movimiento A.C.)

Manipulación masiva con noticias falsas o *fake news*

La desinformación no es un fenñomeno nuevo, lo que es inédito es la velocidad y la amplitud con la que se propaga toda clase de bulos, informaciones trucadas o fake news por las redes.

(Fuente: UNESCO)

Fuente: Elaboración propia con datos de INCIBE, OSI y Agencia Española de Protección de Datos Personales. Consultado en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-y-seguridad-en-internet.pdf

10.1. *Grooming*

El *grooming* es una acción ilícita que consiste en que una persona adulta, ocultando su identidad o aparentando ser alguien de una edad parecida a la de su víctima busca ganarse la confianza de una niña, niño o adolescente con la finalidad de obtener fotografías o videos de contenido sexual de carácter sexual. Con este material, El adulto solicita más fotografías, videos o encuentros con fines sexuales, amenazando a la niña, niño o adolescente con publicar sus fotografías y videos o contar sus conversaciones.[61]

El *grooming* consiste en que "un adulto se hace pasar por un menor en internet o intenta establecer contacto con niños y adolescentes que dé pie a una relación de confianza, pasando después al control emocional y, finalmente al chantaje con fines sexuales".[62]

En caso de que una niña, un niño o adolescente sea víctima de grooming, se debe denunciar ante las autoridades competentes ya que se trata de una acción ilícita. Por tanto, sus padres o tutores, así como otras personas que puedan tener conocimiento de este tipo de acciones, deben ofrecer ayuda a los menores para evitar que puedan sufrir daños.

Las redes sociales y otros servicios digitales son utilizados por actores maliciosos con la finalidad de llevar a cabo este tipo de acciones y causar daños a sus víctimas.

10.2. *Sexting*

El *sexting* es una acción que puede causar daños a una niña, un niño o adolescente e incluso ser utilizada posteriormente con fines ilícitos. Consiste en "hacerse fotografías, grabarse en un video o audio, o dejar que lo hagan otros, en una situación comprometida o íntima".[63]

El riesgo es hacer que las víctimas se sientan avergonzadas para que el delincuente las amenace con hacer público el material sexual, causando un grave daño a la persona. Las fotografías, videos o audios pueden ser utilizados posteriormente para amenazar o coaccionar a la víctima. Es decir, puede dar lugar a una sextorsión,

que consiste en “una forma de chantaje en el que el atacante amenaza a la víctima para que realice algún tipo de acción específica con el fin de no hacer públicas imágenes o videos con connotación sexual, que previamente le ha enviado”.[64]

Si un menor recibe una fotografía, video o audio de este tipo, la recomendación es que nunca la envíe o comparta de alguna manera en redes sociales u otros servicios digitales, por ejemplo, en páginas web, blogs o redes sociales.

10.3. *Ciberbullying*

El *ciberbullying* o ciberacoso[65] es cuando un menor, amenaza, humilla o lleva a cabo una acción similar contra otra niña, niño o adolescente que puede “causar graves consecuencias a la persona acosada, desde hacerle sentir mal hasta llegar al suicidio”.[66]

10.4. Manipulación masiva con noticias falsas o *fake news*

Las noticias falsas o *fake news* no son algo nuevo, pero últimamente, gracias al auge de las redes sociales, se han convertido en un gran riesgo para las personas poco informadas que no hacen un uso seguro de los servicios digitales disponibles en internet.

Casi todos hemos leído una noticia falsa en Twitter, en un blog, página web o correo electrónico. La desinformación afecta a todos los ámbitos, desde la política hasta la salud. Durante la pandemia por Covid-19 las *fake news* fueron usadas por personas maliciosas con la finalidad de engañar a una multitud de víctimas. La Organización de Naciones Unidas (ONU)[67] ha indicado que la campaña de desinformación “representan una amenaza para el periodismo basado en los hechos y, particularmente durante la pandemia actual, para la vida de las personas” y que “cualquier falsedad que gane fuerza puede anular la importancia de un conjunto de hechos verdaderos”.

Con la finalidad de evitar la manipulación masiva, en la 27 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Montreux, Suiza, del 14 al 16 de septiembre de

2005, se expresó que “es necesario proteger los derechos y libertades fundamentales de los interesados y evitar, con las medidas adecuadas, las intrusiones, daños y costes injustificados para los mismos, en concreto los efectos negativos y posibles discriminaciones en su esfera personal, así como su renuncia a algunas formas de participación política”.[68]

Relacionado con este tipo de manipulación masiva también existen las depp fakes, que son “videos manipulados para hacer creer a los usuarios que ven a una determinada persona, tanto si es anónima como si es personaje público, realizando declaraciones o acciones que nunca ocurrieron. Para la creación de dichos videos, se utilizan herramientas o programas dotados de tecnología de inteligencia artificial que permiten el intercambio de rostros en imágenes y la modificación de la voz”.[69]

11. Recomendaciones específicas aplicables a situaciones de pandemia como la ocasionada por el Covid-19

Es muy importante seguir determinados lineamientos en el entorno electrónico para afrontar situaciones como la pandemia por Covi-19. Estas recomendaciones también pueden aplicarse en el futuro:

Recomendaciones para proteger los datos personales en redes sociales durante situaciones de pandemia
1. Los usuarios no deben compartir datos personales que puedan suponer un riesgo, tales como número de teléfono, dirección, fotografías o videos en los que se vea su casa.
2. No publicar datos de familiares (nombres y apellidos o fotografía) excepto cuando sea seguro y no ponga en riesgo sus familiares.
3. No publicar datos relativos a la salud ya que la persona usuaria no sabe quién los puede estar viendo y cómo los podría utilizar.
4. Tener cuidado con las campañas de *phishing*, pues un actor malicioso puede enviar un correo electrónico que simula ser de una empresa, organización o entidad confiable y que tiene por objeto engañar a la persona que lo recibe para obtener su nombre de usuario y contraseña de su cuenta bancaria, correo electrónico u otro servicio digital.
5. Utilizar el doble factor de autenicación para acceder a la red social para evitar que una tercera persona no autorizada pueda acceder utilizando el nombre de usuario y contraseña.
6. Comprobar siempre la fuente de una noticia u otra información, ya que hay personas malintencionadas que publican noticias falsas o *fake news* en las redes sociales.
7. Tener cuidado con las solicitudes de amistad si no se conoce a la persona que la ha enviado ya que se podría dar acceso a la lista de conexiones a actores malintencionados que buscan robar datos personales o llevar a cabo acciones ilícitas o fraudes.

Hace algunos años, el Grupo de trabajo del artículo 29 en la Unión Europea hizo el siguiente resumen sobre los derechos y obligaciones de los usuarios de redes sociales:[70]

Aplicabilidad de las directivas comunitarias

1. La Directiva relativa a la protección de datos se aplica generalmente al tratamiento de datos personales por los SRS, aunque su sede se encuentre fuera del EEE.
2. Los proveedores de SRS se consideran responsables del tratamiento de datos en virtud de la Directiva relativa a la protección de datos.
3. Los proveedores de aplicaciones pueden eventualmente ser considerados responsables del tratamiento de datos en virtud de la Directiva relativa a la protección de datos.
4. Los usuarios se consideran interesados por lo que respecta al tratamiento de sus datos por los SRS.
5. El tratamiento de datos personales por los usuarios corresponde en la mayoría de los casos a la exención doméstica. Existen casos en que las actividades de un usuario no se benefician de esta exención.
6. Los SRS no entran en el ámbito de aplicación de la definición de los servicios de comunicaciones electrónicas, y por tanto la Directiva sobre conservación de datos no se aplica a los SRS.

Obligaciones de los SRS

7. Los SRS deberían informar a los usuarios de su identidad y proporcionarles información clara y completa sobre las finalidades y las distintas maneras en que van a tratar los datos personales.
8. Los SRS deberían establecer parámetros por defecto respetuosos de la intimidad.
9. Los SRS deberían informar y advertir a sus usuarios frente a los riesgos de atentado a la intimidad cuando transfieren datos a los SRS.

11. Los SRS deberían recomendar a sus usuarios no poner en línea imágenes o información relativa a otras personas sin el consentimiento de éstas.
12. Como mínimo, en la página inicial de los SRS debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos.
13. La actividad comercial debe ajustarse a las normas establecidas por la Directiva relativa a la protección de datos y la Directiva sobre la protección de la vida privada en el sector de las comunicaciones electrónicas.
14. Los SRS deben establecer plazos máximos de conservación de los datos de los usuarios inactivos. Las cuentas abandonadas deben suprimirse.
15. Por lo que se refiere a los menores, los SRS deberían adoptar medidas adecuadas con el fin de limitar los riesgos.

Derechos de los usuarios

16. Tanto los miembros como los no miembros de los SRS tienen los derechos de los interesados si procede, de acuerdo con las disposiciones de los artículos 10 a 14 de la Directiva relativa a la protección de datos.
17. Tanto los miembros como los no miembros deberían tener acceso a un procedimiento de tratamiento de las denuncias establecido por los SRS y de fácil uso.
18. Los usuarios deberían, en general, poder adoptar un seudónimo.

Ante la rápida evolución de las redes sociales y otros servicios digitales durante los últimos años, es inexcusable hacer las siguientes recomendaciones para proteger los datos y la privacidad de las partes interesadas:

	**Persona usuaria** - Antes de hacer uso de redes sociales, es necesario conocer dónde está la empresa que las ofrece, su modelo de negocio (mercadotecnia, venta de datos personales, etcétera), qué datos personales trata y para qué. - Leer aviso de privacidad. - En todo momento, revisar sus preferencias de protección de datos y privacidad.
	**Autoridad de protección de datos** - Cooperar con otras autoridades de protección de datos y privacidadd, tanto en foros internacionales como a través de mecanismos de cooperación, para garantizar el derecho humano a la protección de datos personales. - Promover acciones en colaboración con la industria con la finalidad de que las personas usuarias conozcan sus derechos y eviten riesgos derivados de acciones ilícitas o maliciosas a terceros.
	**Otras autoridades competentes** - Adoptar mecanismos de colaboración (convenios o acuerdos) con otras autoridades para prevenir y evitar ciberdelitos u otras acciones ilícitas. - Proporcionar a las personas usuarias recomendaciones y alertas sobre ciberdelitos.
	**Industria y academia** - En el caso de la industria, desarrollar productos y servicios digitales que protejan la privacidad por defecto y faciliten el control por la persona usuaria de sus datos personales. - La academia puede desempeñar un papel relevante a través de la concientización sobre derechos de la persona y su aplicación en internet.

Fuente: Elaboración propia con datos de Grupo de Trabajo, artículo 29. Consultado en: https://goo.su/SMZOxhJ

Conclusiones

Para finalizar, presentamos una lista con las principales conclusiones sobre la privacidad en la era de las redes sociales:

1. La constante y rápida evolución de la tecnología y los servicios digitales, tales como las redes sociales, implican que la privacidad esté también en constante cambio.
2. La privacidad no es el único derecho que la persona usuaria de redes sociales debe tener en cuenta. Cuando una persona hace uso de las redes sociales sus derechos a la protección de datos personales y al secreto de las comunicaciones se ven también expuestos a posibles riesgos y amenazas.
3. El derecho a la protección de datos personales significa que la persona usuaria de una red social u otros servicios digitales, tales como las aplicaciones o *apps* debe tener el control sobre el tratamiento y uso de sus datos personales.
4. El derecho a la privacidad permite a la persona usuaria proteger su esfera más íntima o vida privada.
5. El derecho al secreto de las comunicaciones protege el contenido de los correos electrónicos o mensajes privados que se envían a través de una red privada frente a terceros no autorizados.
6. Una red social es un servicio digital que permite a una persona usuaria acceder a contenidos de su interés, comunicarse con otras personas como familiares, amigos, empresas u otras

organizaciones, publicar y compartir contenidos o realizar cualesquiera otras acciones, tales como la compra de productos o servicios. Existen multitud de tipos o clases de redes sociales.

7. Según las cifras del INAI, las cinco redes sociales más utilizadas en México en 2021 fueron Facebook, WhatsApp, Twitter, YouTube e Instagram.
8. El Instituto Federal de Telecomunicaciones, en su estudio *Privacidad de la Información de los Usuarios en el Uso de Servicios Digitales, México* destacó que "las redes sociales son los servicios digitales que más información recopilan de los usuarios".
9. Según el estudio de We are social, en febrero de 2022 en México 102.5 millones de personas hacían uso de las redes sociales, lo que representaba el 78.3 por ciento de la población mexicana activa en internet. Esta cifra supone un incremento de más de 2.5 millones de personas usuarias de redes sociales, es decir, el 2.5 por ciento de incremento entre 2021 y 2022. Es decir, que cada vez más mexicanos usan las redes sociales.
10. La persona titular de los datos es la persona usuaria de quien se tratan datos personales. El responsable del tratamiento es la persona física o moral que presta el servicio de red social. Los terceros son otros responsables del tratamiento que ofrecen aplicaciones a través de las redes sociales y ofrecen publicidad o usan los datos personales de los usuarios para hacer estudios. El encargado del tratamiento puede ser también la red social cuando permite a una empresa crear una página de fans o utilizarla para vender productos o servicios.
11. Una red social puede tratar una multitud de datos personales sobre una persona usuaria, lo que puede incluir datos personales sensibles, tales como los relativos a la salud, religión o preferencia sexual.
12. La persona usuaria de quien se tratan datos personales puede ejercer sus derechos en protección de datos solicitando el

acceso para conocer qué datos personales trata la red social; la rectificación de los datos personales inexactos o incompletos; la cancelación de los datos personales que ya no son necesarios o que se tratan incumpliendo la normatividad sobre protección de datos o solicitar oponerse al tratamiento de los datos personales cuando existe una causa legítima derivada de una situación personal.

13. Cuando se hace uso de una red social es necesario actuar con precaución y considerar que pueden existir riesgos como la manipulación masiva, la desinformación, las noticias falsas o *fake news* y las acciones ilícitas como el *grooming,* el *ciberbullying* o el *sexting.*

14. Se debe tener en cuenta que ninguna información en línea es privada, y que todos los usuarios de internet pueden recibir correos electrónicos que buscan robar (*phishing*) datos personales como el nombre del usuario y contraseña. Por eso, es importante configurar las preferencias de privacidad para controlar quién ve las imágenes o contenidos que se publican en una red social.

15. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), los órganos garantes a nivel estatal y las autoridades de protección de datos internacionales deben coadyuvar a garantizar el derecho fundamental a la protección de datos personales. Otros sujetos relevantes son las autoridades competentes como la policía, quienes pueden ayudar y colaborar con dichas autoridades para prevenir y evitar ciberdelitos u otras acciones ilícitas o maliciosas.

16. Cualquier actividad en redes sociales puede ser conocida por otras personas, de manera que es necesario cuidar lo que se hace para evitar que una acción puede tener consecuencias negativas como la pérdida de oportunidades laborales o daños a terceros.

17. La privacidad evoluciona a la par de la tecnología y los servicios digitales como las redes sociales, por lo tanto, es necesario

que los usuarios sean conscientes de su titularidad sobre los derechos de protección de sus datos personales, a la privacidad y al secreto de las comunicaciones. Un uso informado y responsable de las redes sociales puede ayudarlos a obtener el su máximo beneficio y evitar los riesgos derivados de estar expuestos a acciones maliciosas o ilícitas.

Glosario de términos

- **Antivirus:** software que tiene como propósito detectar y eliminar *malware.*[71]
- **Aplicación o *app*:** software que puede ser instalado en dispositivos móviles y que fue diseñado para facilitar al usuario la ejecución de una tarea.[72]
- **Ataque de fuerza bruta:** es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta. Este ataque usa el método de prueba y error. Es muy tardado, y por esta razón suele combinarse con otro método llamado ataque de diccionario.[73]
- **Autenticación:** proceso mediante el cual un equipo de cómputo, dispositivo móvil, programa, aplicación o servicio corrobora la identidad de un usuario.[74]
- **Aviso de privacidad:** documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la LFPDPPP (artículo 3.I de la LFPDPPP).
- **Borrado seguro:** medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.[75]

- **Bulo:** mensaje falso muy llamativo que tiene la misión de difundir mentiras, de visitar una web maliciosa o de recopilar direcciones de correo. Pueden ser correos electrónicos, SMS o mensajería instantánea.[76]
- **Captcha:** acrónimo en inglés de Completely Automated Public Turing Test to Tell Computers and Humans Apart. En español, la prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos. Es un tipo de medida de seguridad que consiste en la realización de pruebas —de desafío y respuesta— controladas por máquinas que sirven para determinar cuándo el usuario es un humano o un bot.[77]
- **Ciberataque:** intento deliberado de un ciberdelincuente para obtener el acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos como el robo de información, extorsión del propietario o simplemente daños al sistema.[78]
- **Ciberdelincuente:** persona que realiza actividades delictivas en la red contra personas o sistemas informáticos causando daños económicos o reputacionales mediante el robo, filtración de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.[79]
- **Cifrado:** medida de seguridad para proteger la confidencialidad, la cual codifica la información a través de un algoritmo y una clave para hacerla legible o ilegible.[80]
- **Cifrado de extremo a extremo:** es la propiedad de algunos sistemas de comunicación que hace que los mensajes intercambiados sean ilegibles durante la comunicación en caso de interceptación al estar cifrados. Al ser de extremo a extremo, implica que solo el emisor y el receptor podrán descifrar y conocer el contenido del mensaje.[81]
- ***Cookies:*** paquetes de información definidos por un sitio web y almacenados por un navegador de forma automática en el dispositivo del usuario cuando éste visita dicho sitio.[82]

- **Confidencialidad:** es la propiedad de la información por la que se garantiza que está accesible únicamente al personal autorizado. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.[83]
- **Consentimiento:** manifestación de la voluntad del titular de los datos mediante la cual se efectúa su tratamiento (artículo 3.IV de la LFPDPPP).
- **Contraseña o clave:** medida de seguridad para controlar el acceso a un equipo de cómputo, dispositivo móvil, programa, aplicación o servicio a través de una palabra, frase o un conjunto de caracteres alfanuméricos. Las contraseñas basadas solo en números se conocen como PIN, mientras que las basadas en varias palabras o frases tienen el nombre de *passphrase.*[84]
- **Contraseña débil:** tipo de contraseña que se caracteriza por ser corta y haber sido generada por defecto o mediante el uso de nombres propios, variaciones del nombre del usuario o fechas significativas. Son contraseñas que pueden adivinarse de forma rápida mediante el uso de diccionarios.[85]
- **Contraseña robusta:** tipo de contraseña que se caracteriza por ser suficientemente larga, que se crea al azar o mediante la combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, números y caracteres especiales) que dificultan de forma clara su revelación o que se requiera mucho tiempo de cálculo para lograrlo.[86]
- **Control parental:** conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de internet. Estas herramientas tienen la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas determinados por el administrador de la cuenta, que normalmente deberá ser el padre o tutor del menor.[87]

- **Correo de suplantación:** mensaje de correo electrónico, en teoría legítimo, que usa el nombre de una persona u organismo de confianza con el objetivo de obtener información confidencial o personal de la persona u organización a la que se ha enviado.[88]
- **Correo *spam:*** correo electrónico que no fue solicitado por el receptor y que se envía en grandes cantidades con fines publicitarios o como complemento de actividades maliciosas, por ejemplo, los ataques de *phishing*.[89]
- **Datos personales:** cualquier información concerniente a una persona física identificada o identificable (artículo 3.V de la LFPDPPP). Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información. Son ejemplos de datos personales el nombre, los apellidos, la dirección postal, el número de teléfono o de celular, la dirección de correo electrónico, el número de pasaporte, la fotografía, la Clave Única de Registro de Población (CURP), el Registro Federal de Contribuyentes (RFC), los datos de salud y financieros, entre otros.[90]
- **Datos personales sensibles:** son aquellos datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida puede dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual (artículo 3.VI de la LFPDPPP).
- **Derechos ARCO:** derechos de acceso, rectificación, cancelación y oposición.
- **Dirección IP:** número con el que se identifica a los dispositivos electrónicos que están conectados en una red, la cual utiliza el protocolo IP (del inglés *internet protocol*).[91]

- **Dispositivo móvil:** aparato pequeño que cuenta con tecnología de cómputo y acceso a internet, es portable y se puede conectar a un equipo de cómputo para ver su contenido, por ejemplo, teléfonos inteligentes y tabletas.[92]
- **DNS:** del inglés *Domain Name Service,* se refiere tanto al servicio de nombres de dominio, como al servidor que ofrece dicho servicio. El servicio DNS asocia un nombre de dominio con información variada relacionada con ese dominio. Su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de localizar y direccionar estos sistemas de una forma mucho más simple.[93]
- **Equipo de cómputo:** dispositivo electrónico para procesar y almacenar información, está compuesto por hardware, software y dispositivos periféricos.[94]
- **Filtro o control de contenido:** programa que permite limitar el acceso a contenido no deseado al navegar en internet. Por ejemplo, sitios web para adultos, publicitarios o de descargas ilegales.[95]
- **Firewall:** sistema o programa para proteger redes, equipos de cómputo y dispositivos móviles contra intrusiones provenientes de terceros (generalmente desde internet).[96]
- **HTTPS:** es el protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, del inglés *Hypertext Transfer Protocol Secure*, es un protocolo de red destinado a la transferencia segura de datos de hipertexto. Dicho en otras palabras, es la versión segura de HTTP. Es cifrado mediante un algoritmo simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor. Es utilizado para cualquier tipo de servicio que requiera el envío de datos personales o contraseñas, entidades bancarias, tiendas en línea, pago seguro, etcétera.[97]
- **INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

- **Ingeniería social:** conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas o servicios de las TIC. Estas técnicas les facilitan datos de valor, ya sean credenciales, información sobre los sistemas o servicios instalados.[98]
- **Integridad:** la integridad es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados para asegurar que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones clave en la seguridad de la información, ya que se pretende evitar los accesos no autorizados a los datos y garantizar la no alteración de estos.[99]
- **LFPDPPP:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- ***Malware* o software malicioso:** término que engloba a todo tipo de programa o código malicioso cuyas funciones pueden variar desde extraer, borrar e incluso "secuestrar" la información en equipos de cómputo o generar mal funcionamiento en los sistemas. Algunos ejemplos de *malware* son los virus, los troyanos, los gusanos y el *ramsomware*.[100]
- **Mensajería instantánea:** comunicación en tiempo real mediante mensajes de texto, audio o video. Algunas de las aplicaciones de mensajería instantánea son Whatsapp, Facebook Messenger, Skype, Telegram, Line, Viber, Snapchat y WeChat.[101]
- **Metadatos:** los metadatos son el conjunto de datos relacionados con un documento que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos son información que enriquece el documento al que está asociado. A modo de ejemplo, se podría considerar como una analogía al uso de índices que se emplean en una biblioteca, donde gracias a datos del tipo: autor, títulos, etcétera, se permite localizar un libro en

concreto. También se usan para mejorar las consultas en los buscadores y obtener una mayor exactitud y precisión en los resultados.[102]

- **Obtener los datos personales de forma directa de su titular:** acto en el cual el propio titular proporciona los datos personales por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, internet o vía telefónica, entre otros.[103]
- **Obtener los datos personales de forma indirecta:** acto en el cual el responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, por ejemplo a través de una fuente de acceso público o una transferencia.[104]
- ***Phishing:*** técnica o tipo de ataque en el que alguien suplanta a una entidad o servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo o mensaje suele tener un enlace o fichero que contiene un enlace a un sitio web que suplanta al legítimo y que usan para engañarlo.[105]
- ***Ransomware:*** *malware* cuya funcionalidad es "secuestrar" un dispositivo (en sus inicios) o la información que contiene de forma tal que si la víctima no paga el rescate, no podrá acceder a ella.[106]
- **Responsable del tratamiento:** persona física o moral de carácter privado que decide sobre el tratamiento de datos personales (artículo 3.XIV de la LFPDPPP).
- **Robo de identidad:** es la apropiación de la identidad de una persona para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados a fin de obtener ciertos recursos o beneficios a su nombre. El robo de identidad implica la obtención y uso no autorizado e ilegal de datos personales.[107]

- **Titular:** la persona física a quien corresponden los datos personales (artículo 3.XVII de la LFPDPPP).
- **Tratamiento:** la obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales (artículo 3.XVIII de la LFPDPPP).
- **Web *beacons:*** imagen visible u oculta insertada dentro de un sitio web o correo electrónico que se utiliza para monitorear el comportamiento del usuario en estos medios. A través de éstos se puede obtener información como la dirección IP de origen, navegador utilizado, sistema operativo, momento en que se accedió a la página, y en el caso del correo electrónico, la asociación de los datos anteriores con el destinatario.[108]

Bibliografía

- Agencia Española de Protección de Datos. (2019). *Protección de datos y prevención de delitos.* AEPD.
- American Chamber México. (s.f.). *Estrategia de ciberseguridad en México. Por un futuro ciberseguro.* https://cutt.ly/gXsZLwV
- Banco Interamericano de Desarrollo. (2020). *Ciberseguridad, Riesgos, Avances y el Camino a seguir en América Latina y el Caribe, Reporte Ciberseguridad 2020.* https://cutt.ly/tXsBXZY
- Grupo de Trabajo del artículo 29. (2009). *Dictamen 5/2009 sobre las redes sociales en línea (WP 163), adoptado el 12 de junio de 2009.* https://cutt.ly/uXaVr0f
- Instituto Nacional de Ciberseguridad. (2020). *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario,* segunda versión. Instituto Nacional de Ciberseguridad.
- Instituto Nacional de Ciberseguridad y Oficina de Seguridad del Internauta. (2021). *Guía de ciberataques. Todo lo que necesitas saber a nivel usuario.* Incibe.
- Instituto Nacional de Tecnologías de la Comunicación y Agencia Española de Protección de Datos. (2019, febrero). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.* https://www.uv.es/limprot/boletin9/inteco.pdf

- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2018, agosto). *Guía para la configuración de privacidad en redes sociales.* INAI.
- _____. (s.f.). *Guía para prevenir el robo de identidad.* INAI. https://cutt.ly/PXfASpo
- _____. (2018, marzo). *Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital.* INAI. https://cutt.ly/uXfA49l
- _____. (2018, junio). *Procedimiento para ejercer los Derechos ARCO.* INAI. https://cutt.ly/5XfSfrO
- _____. (2019, mayo). *Herramientas o aplicaciones de Supervisión Parental en Internet.* INAI. https://cutt.ly/yXfSA17
- Piñar, J. L. (2011). *Redes sociales y privacidad del menor.* Reus.
- Ponce, I. (2012). *Monográfico Redes Sociales.* Ministerio de Educación del Gobierno de España.
- Recio, M. (Coord.). (2016). *La Constitución en la sociedad y economía digitales, Temas selectos de derecho digital mexicano.* Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación.

Citas bibliográficas

1. Piñar , J. L. y Recio , M. (2016). “La privacidad en Internet”, en Recio Gayo, Miguel (Coord.). *La Constitución en la sociedad y economía digitales. Temas selectos de derecho digital mexicano.* Centro de Estudios Constitucionales de la Suprema Corte de Justicia de la Nación, pp. 82. https://cutt.ly/VXaZmQf
2. Grupo de Trabajo del artículo 29. (1997). *Recomendación 3/97, Anonimato en Internet (WP 6), adoptada el 3 de diciembre de 1997.* https://cutt.ly/UXaZ7oW
3. El párrafo segundo del artículo 16 constitucional indica que “Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.”
4. “El párrafo primero del artículo 16 constitucional indica que “Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la orali-

dad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo."

5. Ponce, I. (2012). *Monográfico Redes Sociales.* Ministerio de Educación del Gobierno de España, p .2. https://cutt.ly/VXaC0rW
6. Real Academia Española. *Diccionario de la lengua española.* https://dle.rae.es/red#GExglxC
7. Real Academia Española. *Diccionario Panhispánico del Español Jurídico.* https://dpej.rae.es/lema/red-social
8. Grupo de Trabajo del artículo 29. (2009). *Dictamen 5/2009 sobre las redes sociales en línea (WP 163), adoptado el 12 de junio de 2009*, p . 5. https://cutt.ly/uXaVr0f
9. Ibidem, pág. 5.
10. Instituto Nacional de Tecnologías de la Comunicación y Agencia Española de Protección de Datos. (2019, febrero). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online,* p.7. https://www.uv.es/limprot/boletin9/inteco.pdf
11. Cifras consultadas en enero de 2022 en https://www.inegi.org.mx/temas/ticshogares/
12. INAI. (2018, marzo). *Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital,* op. cit., pág. 20.
13. Asociación de Internet mx. (2022, mayo). 18º *Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022.* https://cutt.ly/YXaNHjc
14. Ibid.
15. Instituto Federal de Telecomunicaciones (IFT). (s.f.). *Privacidad de la Información de los Usuarios en el Uso de Servicios Digitales,* p.14. https://cutt.ly/VXaMvQa

16. Según los datos publicados por We are social en https://datareportal.com/reports/digital-2022-mexico
17. Consultado en https://datareportal.com/reports/digital-2022-mexico
18. Fuente: https://cutt.ly/qXa1MnF
19. Observatorio Nacional de Tecnología y Sociedad (Ontsi). (2011, diciembre). *Las Redes Sociales en Internet,* p . 13 y siguientes. https://cutt.ly/5Xa0GiN
20. Ontsi, op. cit., pág. 13.
21. Ontsi, op. cit., págs. 13 y 14.
22. Ontsi, op. cit., pág. 16.
23. Ibidem , pág. 16.
24. Ibidem, pág. 16.
25. Ibidem, pág. 17.
26. Ibidem, pág. 17.
27. Ponce, I. (2012). *Monográfico Redes Sociales.* Ministerio de Educación del Gobierno, p. 4.
28. Ibidem, pág. 4.
29. Ibid.
30. Ibid.
31. Instituto Nacional de Transparencia, *Acceso a la Información y Protección de Datos Personales. (s.f.) Guía para Titulares de los Datos Personales, Volumen 1.* https://cutt.ly/jXswljt
32. INAI (s.f.). *Guía para Titulares de los Datos Personales,* op. cit, pág. 10.
33. Piñar, J. L. (2011). *Redes sociales y privacidad del menor.* Reus, p. 16.
34. Piñar, J. L. y Recio , M. “La privacidad en Internet”, op. cit., p . 78.

35. Recomendaciones adoptadas en el Seminario Derechos, Adolescentes y Redes Sociales en Internet realizado en Montevideo, Uruguay del 27 y 28 de julio de 2009. https://programainfancia.uam.mx/pdf/s_doc/biblioteca/memorandum_montevideo.pdf
36. Grupo de Trabajo del artículo 29, op. cit., p . 5.
37. Págs. 21 a 33.
38. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) define al tercero como: "La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos" (artículo 3.XVI).
39. Es definido en la LFPDPPP como la "persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable" (artículo 3.IX de la LFPDPPP).
40. Instituto Federal de Telecomunicaciones. *Privacidad de la Información de los Usuarios* …, op. cit., p. 18 y siguientes.
41. Definición del artículo 3. XVIII de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
42. El soporte físico es definido como un "medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales" (artículo 2.XI del Reglamento de la LFPDPPP).
43. Un soporte electrónico es un "medio de almacenamiento al que se pueda acceder so lo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms" (artículo 2.X del Reglamento de la LFPDPPP).
44. Artículo 3 del Reglamento de la LFPDPPP.
45. INAI. (2018). *Guía para Titulares de los Datos Personales,* op. cit., p. 10.

46. Comité Europeo de Protección de Datos. (2021). *Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, Versión 2.0, adoptadas el 13 de abril de 2021,* p . 8. https://cutt.ly/jXssru0
47. Ibidem, pág. 9.
48. Ibidem, pág. 7.
49. Ibid.
50. Parra, L. G . (s.f.). *Redes sociales y protección de datos personales.* INAI, p. 5. https://cutt.ly/nXszuBG
51. Ontisi , op. cit., pág. 93.
52. Inteco y Agencia Española de Protección de Datos, op. cit., p. 11 y 12.
53. Inteco y Agencia Española de Protección de Datos, op. cit., págs. 19 a 21.
54. Ibidem, págs. 144 a 147.
55. Agencia Española de Protección de Datos e Instituto Nacional de Ciberseguridad y Oficina de Seguridad del Internauta. (2019). *Privacidad y Seguridad en Internet,* p . 12. https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-y-seguridad-en-internet.pdf
56. American Chamber México. (s.f.). Estrategia de ciberseguridad en México. *Por un futuro ciberseguro,* p. 4. https://cutt.ly/gXsZLwV
57. INAI. (s.f.). *Guía para prevenir el robo de identidad*, p. 13.
58. Banco Interamericano de Desarrollo. (2020). *Ciberseguridad, Riesgos, Avances y el Camino a seguir en América Latina y el Caribe, Reporte Ciberseguridad 2020,* p. 125. https://cutt.ly/tXsBXZY
59. Ibidem, pág. 126.
60. INAI. (s.f.). Guía para prevenir el robo de identidad, op. cit., pp. 12 y 13.

61. La Agencia Española de Protección de Datos se refiere al *grooming* de la siguiente manera: “Cuando un adulto, a través de las redes sociales u otros servicios de internet, oculta su identidad, generalmente haciéndose pasar por un menor, con el objetivo de ganarse la confianza de otro menor.

62. En ocasiones, el adulto accede a la información personal del menor sobre sus gustos, hábitos y aficiones, que utiliza para ganarse su amistad y confianza. Cuando ya se ha ganado su confianza consigue que le cuente cosas o que le envíe fotos o videos de actos o comportamientos comprometidos y de contenido sexual. Una vez obtenida esta información, le pide más fotografías o videos o tener encuentros con fines sexuales y, si no se los da o acepta, es cuando le amenaza con contar lo que le ha dicho o con publicar las fotos y videos que le envió”. Agencia Española de Protección de Datos. (2019). *Protección de datos y prevención de delitos,* p. 2. https://cutt.ly/fXdNHW4

63. Instituto Nacional de Ciberseguridad. (s.f.). *Grooming, amistades muy peligrosas.* Incibe. https://www.incibe.es/aprendeciberseguridad/grooming

64. Agencia Española de Protección de Datos. (2019). *Protección de datos y prevención de delitos*, op. cit., p. 1.

65. Incibe. (s.f.). Sextorsión, protege tu intimidad y evitarás chantajes. https://www.incibe.es/aprendeciberseguridad/sextorsion

66. La Agencia Española de Protección de Datos ha indicado sobre el ciberbullying que se trata de “amenazas, hostigamiento, humillación, control u otro tipo de molestias realizadas por un adulto contra otra persona por medio de las tecnologías de la información y comunicación (internet). Cuando se produce entre menores se conoce como ciberbullying”. El acoso a través de internet, a diferencia del acoso físico, supera las barreras del espacio y del tiempo. Se puede producir a cualquier hora del día y con independencia del lugar donde se encuentre el acosado.” Agencia Española de Protección de Datos, op cit., p. 3.

67. Ibid.

68. Organización de las Naciones Unidas. (2020). *Noticias falsas y desinformación, otra pandemia del coronavirus.* ONU. https://news.un.org/es/story/2020/04/1472922

69. 27 Conferencia Internacional de la Asamblea Global de Privacidad. (2005). *Resolución sobre el Uso de Datos Personales para la Comunicación Política, Montreux* (Suiza), 14 a 16 de septiembre de 2005. https://cutt.ly/eXd06iG

70. Instituto Nacional de Ciberseguridad. (s.f.). *Deep Fakes, Las apariencias engañan.* https://www.incibe.es/aprendeciberseguridad/deepfakes

71. *Op. cit.*, págs. 13 y 14.

72. INAI. (2018, marzo). *Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital* op. cit., p . 4.

73. Ibidem, pág. 4.

74. Instituto Nacional de Ciberseguridad. (2020). *Glosario de términos de ciberseguridad: una aproximación para el empresario,* op. cit., p. 16.

75. INAI. (2018, marzo). *Recomendaciones para mantener segura tu privacidad*, op. cit., p. 4.

76. Ibidem, p. 4.

77. Instituto Nacional de Ciberseguridad. (2020). Glosario de términos de ciberseguridad, op. cit., p. 23.

78. Ibidem , p. 24.

79. Ibidem , p. 27.

80. Ibidem , p. 27.

81. INAI. (marzo, 2018). *Recomendaciones para mantener segura tu privacidad,* op. cit., p. 4.

82. Instituto Nacional de Ciberseguridad. (2020). *Glosario de términos de ciberseguridad,* op. cit., p. 28.

83. INAI. (marzo, 2018). *Recomendaciones para mantener segura tu privacidad,* op. cit., p. 4.
84. Instituto Nacional de Ciberseguridad. (2020). *Glosario de términos de ciberseguridad,* op. cit., p. 30.
85. INAI. (marzo, 2018). Recomendaciones para mantener segura tu privacidad, op. cit., p. 4.
86. Instituto Nacional de Ciberseguridad. (s.f.). *Glosario de términos de ciberseguridad,* op. cit., p. 30.
87. Ibidem, p. 30.
88. Ibidem, p. 31.
89. Ibidem, p. 32.
90. Ibidem, p. 32.
91. INAI. (2018, marzo). *Recomendaciones para mantener segura tu privacidad,* op. cit., p. 5.
92. Ibidem , p. 5.
93. Ibidem , p. 5.
94. Instituto Nacional de Ciberseguridad. (2020). *Glosario de términos de ciberseguridad,* op. cit., p. 39.
95. INAI. (s.f.) . *Recomendaciones para mantener segura tu privacidad,* op. cit., p. 5.
96. Ibidem, p. 5.
97. Ibidem, p. 5.
98. Instituto Nacional de Ciberseguridad. (s.f.). *Glosario de términos de ciberseguridad,* op. cit., p. 49.
99. Ibidem, p. 51.
100. Ibidem, p. 52.
101. INAI. (2018, marzo). *Recomendaciones para mantener segura tu privacidad,* op. cit., p. 5.

102. Ibidem, p. 5.
103. Instituto Nacional de Ciberseguridad. (s.f.). *Glosario de términos de ciberseguridad*, op. cit., p. 57.
104. Lineamiento tercero de los Lineamientos del Aviso de Privacidad.
105. Ibid.
106. Instituto Nacional de Ciberseguridad. (2020). *Glosario de términos de ciberseguridad,* op. cit., p. 61.
107. Ibidem, p. 65.
108. INAI. (s.f.). *Guía para Prevenir el robo de identidad,* p. 5.
109. Lineamiento tercero de los Lineamientos del Aviso de Privacidad.


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