



El ejercicio del **Derecho a la Protección de Datos Personales** y el **Derecho a la Información Pública** como una práctica de autocuidado y seguridad, en redes sociales



Aula Virtual
#ProtejoMisDatos



PRESENTACIÓN



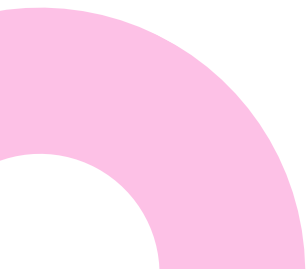
¡Hola, amigas y amigos!

En este espacio conoceremos un poco acerca de la forma en la que podemos ejercer nuestros **derechos de acceso a la información y protección de datos personales**.

Sabemos que te estás preguntando: “pero ¿qué son esos derechos?”. Bueno, son más importantes de lo que te imaginas.

Actualmente, gracias al avance tecnológico y científico, tenemos a nuestra disposición una gran cantidad de información de forma accesible e inmediata.

Por ejemplo, cuando usamos Internet para hacer la tarea o al revisar nuestras redes sociales, podemos conocer sobre distintos temas de México y el mundo, conectarnos con personas a lo largo y ancho del planeta, y realizar muchas actividades como comprar comida, pedir taxis o pagar el teléfono.



¿Sabías que esto permite que exista una gran cantidad de información al alcance de personas, empresas, gobiernos e inclusive, de grupos delincuenciales y criminales?

Bueno, justamente por eso es importante que conozcamos los **derechos de acceso a la información (DAI)** y a la **protección de datos personales (DPDP)**, para que nuestros datos personales y la información pública sean utilizadas de forma informada, responsable y con apego a las leyes.



En este espacio encontrarás la información necesaria para comprender **qué son los datos personales** y **qué es la información pública**, y **ejercer tus derechos**.



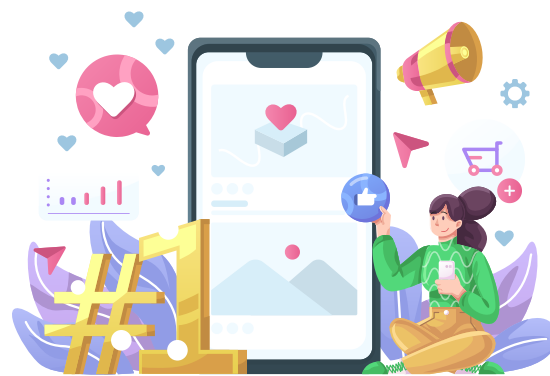
OBJETIVO

Concientizar a jóvenes sobre el ejercicio del derecho a la protección de datos personales, principalmente en redes sociales, como medida de autocuidado y seguridad, para prevenir situaciones de riesgo.



Asimismo, se explicará el proceso a realizar para que la ciudadanía, incluyendo las/os jóvenes, realicen solicitudes de acceso a la información pública a través del sistema INFOMEX-Plataforma Nacional de Transparencia, para el ejercicio de sus derechos de acceso, rectificación, cancelación de datos personales y oposición a su tratamiento (derechos ARCO).

Y lo más importante, en esta aula también se presentarán herramientas sobre cómo proteger datos personales en redes sociales.



ÍNDICE



Introducción. ¿qué es la información pública y que son los datos personales?

I. Derecho de Acceso a la Información Pública (DAIP).

II. Derecho a la Protección de Datos Personales (DPDP). Cómo ejercerlo y qué instancias lo protegen.

III. Cuido mi información.

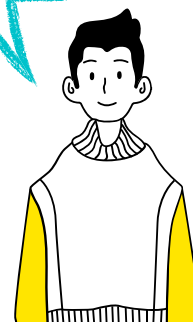


Introducción

¿Qué es la información pública y que son los datos personales?

El artículo 6° de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) , define la **información pública como toda aquella que se encuentra en posesión de las autoridades de los tres poderes de gobierno (Ejecutivo, Legislativo y Judicial), en los tres órdenes de gobierno (Federal, Estatal y Municipal), así como de organismos autónomos, partidos políticos y personas físicas o morales que reciban o ejerzan recursos públicos.**

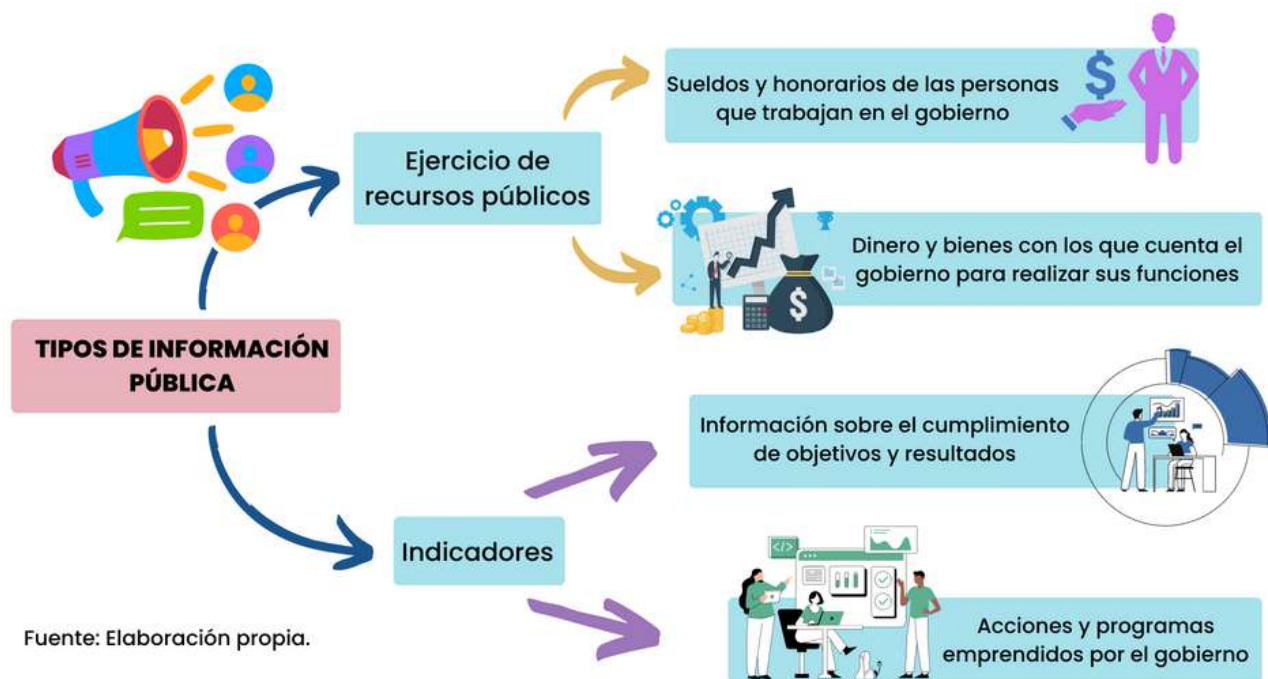
En pocas palabras amigos, la información pública es la información con la que funciona el gobierno.



A continuación te mostramos qué entidades manejan información pública y algunos ejemplos:



Para que todas las personas podamos conocer la información pública, existe el **principio de máxima publicidad**, esto quiere decir que todas las instituciones públicas tienen la obligación de publicar y actualizar información específica. Pero, ¿Qué tipo de información deben actualizar y a la que tenemos derecho de conocer? Te mostramos a continuación:



Fuente: Elaboración propia.

Sin embargo, como pasa en las series de intriga y misterio, **a veces el gobierno no nos dice todo** 🤖 Pero no te asustes ni te enojas, **las instituciones públicas pueden reservar temporalmente información por razones de seguridad nacional e interés público.**

Después del tiempo que establezca el gobierno, la información reservada se abre al público y puede consultarse a través de los diferentes mecanismos que establece la ley, ¿qué te parece?



Por ejemplo, los operativos para combatir a la delincuencia organizada y los datos con los que cuentan las oficinas de inteligencia sobre los criminales pueden ser muy interesantes para escribir una serie policíaca, pero **estos datos pueden poner en peligro la vida, integridad y seguridad**, tanto de la ciudadanía, como de los del personal del Ejército, Marina y Policía, por lo que se suele reservar esta información en el interés de todas y todos.

Un momento...



Los datos personales son toda aquella información que se refiere a la vida privada de las personas, es decir, aquella que únicamente concierne a nosotrxs como individuos, se conoce como datos personales, mismos que utilizamos en nuestra vida cotidiana, por ejemplo, el domicilio en el que vivimos, preferencia sexual, religión, religión, entre otros.

Muchas personas o empresas pueden acceder a nuestros datos personales para celebrar contratos y ofrecernos servicios que hacen nuestra vida más sencilla (pedir comida desde una app) o más entretenida (responder quizzes para saber qué tipo de tostada eres), pero también **existen personas y grupos que aprovechan la gran cantidad de información que está disponible para causarnos daño**, por esta razón existen leyes y el gobierno debe proteger nuestros datos, pero **también nosotras/os debemos ser cuidadosas/os con la información que compartimos**.



La importancia que el **Derechos de Acceso a la Información Pública (DAIP)** y **del Derecho a la Protección de Datos Personales (DPDP)** sean garantizado por las leyes radica en que la información no siempre se pone a disposición de la ciudadanía, mientras que los datos personales pueden ser utilizados sin nuestro consentimiento.

Cualquiera de nosotras/os podemos acceder gratuitamente a la información pública, sin necesidad de que acreditemos el interés que tenemos en ella, ni de justificar el uso que haremos de la misma, al tiempo que podemos solicitar el acceso, rectificación, cancelación y oposición de nuestra información personal que se encuentre en posesión de particulares.



Es importante que sepas que no estamos solas/os. Para ejercer nuestros **derechos** al acceso a la información y protección de datos personales, es necesario que **utilicemos los mecanismos y procedimientos establecidos por las leyes mexicanas**, y que acudamos a la instancia gubernamental por excelencia en la cuestión: **el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)**.



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

Es el organismo autónomo, especializado, imparcial y colegiado de la Administración Pública Federal (APF) que se encarga de **garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales** en posesión de entes públicos y de particulares, así como de la promoción de una **cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales** para el fortalecimiento de una sociedad incluyente y participativa.

Fuente: INAI, Misión, URL: https://home.inai.org.mx/?page_id=1626, consultado el 2 de junio de 2022

El INAI contribuye a que ejerzamos nuestro derecho de acceso a la información y la protección de datos personales, y también nosotras/os podemos hacerlo a través de las herramientas que te daremos a conocer en esta aula.

I. Derecho de Acceso a la Información Pública (DAIP).



Como te comentamos anteriormente, en la Constitución se establece nuestro Derecho de Acceso a la Información, por lo cual, el Estado mexicano debe proveer todo lo necesario para **facilitar el acceso a la información pública** mediante procedimientos sencillos y expeditos, además de que debe **transparentar la gestión del gobierno y propiciar la rendición de cuentas a las/os ciudadanas/os.**

El Derecho de Acceso a la Información se equipara al derecho a la educación o a la salud. ¡Es así de importante!

A graphic with a yellow background and pink accents. It features an icon of an open book and a gavel. The text reads: "Artículo 6°" and "Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión". At the bottom, it says "Fuente: Constitución Política de los Estados Unidos Mexicanos". On the right, there is an illustration of a woman reading a newspaper.

Artículo 6°

"Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión"

Fuente: Constitución Política de los Estados Unidos Mexicanos

Además de que la labor del INAI se rige por el artículo 6° constitucional, también se fundamenta en las siguientes leyes:

Marco normativo del INAI



Con base en las leyes que vimos en la imagen anterior e instituciones como el INAI, no sólo podemos solicitar información, sino que ésta ya debe ser pública debido al **principio de transparencia activa**, la cual consiste en la publicación de información por parte de los sujetos obligados de acuerdo con lo establecido en la Ley.

Los sujetos obligados son todas las dependencias públicas que deben transparentar y permitir el acceso a la información y proteger los datos personales.



Hagamos una pausa, ¿recuerdas que anteriormente mencionamos que hay "información reservada"? la cual se resguarda por seguridad de todas/os, pues también hay otro tipo de información que debe cuidarse: la confidencial.

Revisemos el siguiente cuadro para que no nos confundamos entre una y otra.

Tipos de información que se resguarda	
Reservada	Confidencial
✓ Menoscaba la conducción de negociaciones o relaciones internacionales	Los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal de particulares
✓ Pone en riesgo la vida, seguridad o salud de una persona física	Aquella que presenten los particulares a los sujetos obligados
Puede afectar la efectividad de las políticas monetaria, cambiaria o financiera del país	✓ Contiene datos personales concernientes a una persona física
✓ Compromete la seguridad nacional, la seguridad pública o la defensa nacional	✓
Obstruye la prevención o persecución de delitos	
Afecta los derechos al debido proceso	

Fuente: Secretaría de la Función Pública, Qué es información confidencial, reservada y versión pública. URL: <https://www.gob.mx/sfp/documentos/que-es-informacion-confidencial-informacion-reservada-version-publica>

Entonces ¿nunca podremos conocer la información reservada?

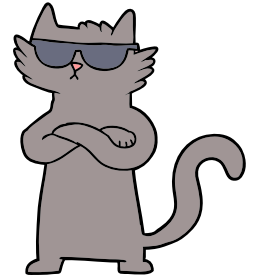
Toda clasificación y reserva de información tiene un plazo de desclasificación de 5 años (que puede ser ampliado por un periodo similar). Entonces, una vez que se vence este plazo, expiran las causas que dieron paso a su clasificación, o cuando una autoridad competente determina que existe una causa de interés público que prevalece sobre la reserva de información, la información se desclasifica y la podemos conocer.



Pero ninguna información puede ser clasificada o reservada si trata de violaciones graves a derechos humanos o delitos de lesa humanidad, o en caso de estar relacionada con actos de corrupción



Además de la **transparencia activa**, contamos con el principio de **transparencia reactiva**, el cual implica que cualquiera de nosotras/os **podemos presentar una solicitud de acceso a información**, sin dar ninguna explicación del por qué la **requerimos**, ni para qué la utilizaremos.



Esto, porque existe **otro tipo de información que usualmente no conocemos**, pero que **podemos solicitar a nuestras autoridades**, ya que se trata de información pública



Así es también podemos conocer estos datos a través de una **solicitud de información**, que es un escrito por el que podemos requerir acceso a información pública que se encuentra en documentos que generen, obtengan, adquieran, transformen o conserven en sus archivos los sujetos obligados por la ley.

Lo podemos hacer a través del **INAI** y de las **Unidades de Transparencia de los sujetos obligados**, específicamente, por medio de la **Plataforma Nacional de Transparencia** disponible en la web (<https://buscador.plataformadetransparencia.org.mx/>), entre otras herramientas como las que te mostramos a continuación:

MEDIOS PARA REALIZAR UNA SOLICITUD DE INFORMACIÓN

1. Por medios electrónicos a través de la Plataforma Nacional de Transparencia o el sistema INFOMEX



2. A través de un formato escrito que se envía por correo certificado o mensajería ante la Unidad de Transparencia de la entidad a la que se solicita la información.



3. Acudiendo personalmente a la Unidad de Transparencia de la entidad a la que se solicita la información, presentando un formato escrito.



Fuente: Elaboración propia.

 **CAVINAI** LLEGA A LA
PLATAFORMA DE TRANSPARENCIA

INGRESA A:
www.plataformadetransparencia.org.mx
Y HAZ CLICK EN LA PESTAÑA



www.inai.org.mx



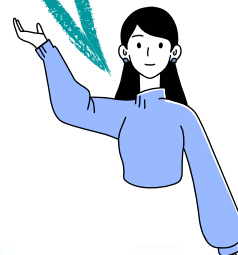
@CAS_inai



atencion@inai.org.mx

Tel inai
800 835 4324

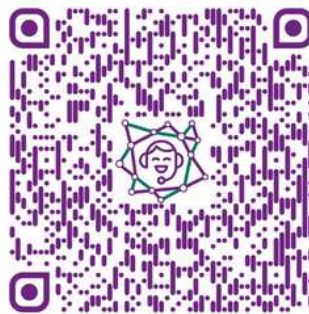
Además de estos medios, también cuentas con el Centro de Atención Virtual (CANVINAI) para realizar tus consultas



¿Tienes una
CONSULTA?



Puedes ingresar a <https://home.inai.org.mx> o escribir al Whatsapp al: 55 5004 2330



Escanea y
escribele a



CAVINAI



www.inai.org.mx

@cas_inai

atencion@inai.org.mx



800 835 4324

También te sugerimos el siguiente video que te orienta paso a paso sobre cómo realizar una solicitud de información a través de la Plataforma Nacional de Transferencia:

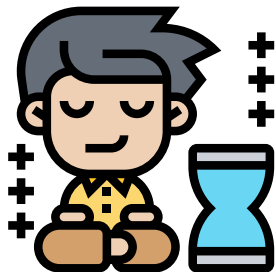
¿Cómo realizar una solicitud de información en la PNT?, INAI, 2019:
<https://youtu.be/cTAyx23jFcl>

Parece que es muy fácil y ¡lo es! pero es importante que nuestras solicitudes de información estén planteadas debidamente y contengan lo que deseamos conocer.

No dudes en consultar a tu papá, mamá o profesores antes de enviar tu solicitud o acércate a nosotras/os a través de las redes sociales de Articulación Ciudadana para la Equidad y el Desarrollo AC

Imagina que tus profesoras/es te preguntarán algo pero no entiendes la pregunta en sí, ¿parece aterrador, verdad?

De este modo, nuestra pregunta debe ser lo más precisa posible, entra más clara sea nuestra solicitud de información, es más probable que la respuesta que recibamos sea más precisa y veloz.





Nuestra solicitud de información debe ser respondida en un plazo no mayor a 20 días hábiles, contados desde que es recibida (conserva tu acuse de recibo), esto cuando realizas solicitudes de información a entidades federales, pero el periodo varía cuando la solicitud es a entidades locales.

Por causas extraordinarias, la respuesta puede tardar un periodo adicional de 20 días hábiles, siempre y cuando las autoridades nos notifiquen de las razones por las cuales se amplía el tiempo de respuesta.

Pero, ¿Qué pasa si no obtenemos ninguna respuesta a nuestra solicitud de información?

Supuestos ante las solicitudes de información

<p>¿Si no responden mi solicitud de información?</p> 	<p>¿Si me niegan información, está incompleta o no corresponde a mi solicitud?</p> 
<p>Podemos presentar una solicitud para verificar la falta de respuesta. De esta forma, el INAI ordena a los sujetos obligados para que entreguen en un plazo no mayor de 10 días hábiles la información solicitada o, cuando sea el caso, avisarnos si la misma se encuentra clasificada como reservada o confidencial.</p>	<p>Podemos presentar en un plazo no mayor de 15 días hábiles desde que se recibe la respuesta, un Recurso de Revisión ante el INAI para que el Pleno del Instituto conozca y resuelva la controversia en un plazo no mayor a 50 días hábiles (puede prorrogarse por 30 días hábiles para la integración del documento y 20 días hábiles para resolver en definitiva).</p>

¿Qué opinas acerca de las herramientas con que cuentas para ejercer tu Derecho de Acceso a la Información (DAI)? ¿Lo imaginabas?

Antes de terminar, debes saber que, además de realizar solicitudes de información específica, la Plataforma Nacional de Transparencia integra una herramienta fantástica que es el buscador donde también puedes encontrar la información que necesitas.



Además de que en la parte inferior de la Plataforma encontrarás información en diferentes ejes temáticos dependiendo de lo que requieras.



En materia de transparencia y rendición de cuentas, además del INAI en el ámbito federal, **cada estado de la República cuenta con una institución que se encarga de instrumentar las acciones y políticas para que ejerzamos nuestro derecho al acceso a la información y protección de datos en el ámbito local.**



Por ejemplo, en **Oaxaca** tenemos al **Instituto de Acceso a la Información Pública y Protección de Datos Personales de Oaxaca (IAIP Oaxaca)**, a través del cual, podemos exigir la protección de nuestros derechos de acceso a la información, así como proteger nuestros datos personales en posesión de particulares domiciliados en Oaxaca.



Instituto de Acceso
a la Información Pública
y Protección de Datos Personales
del Estado de Oaxaca



En 2015, se decidió crear el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en el cual, se integran los 32 órganos locales de transparencia y acceso a la información pública junto al INAI, el Archivo General de la Nación (AGN), la Auditoría Superior de la Federación (ASF) y el Instituto Nacional de Estadística y Geografía (INEGI) para fomentar la coordinación y colaboración interinstitucional y permitir de esta forma, el fortalecimiento de la transparencia y la rendición de cuentas en México, así como garantizar el cumplimiento de los derechos de acceso a la información y protección de datos personales.



Gracias al **Sistema Nacional de Transparencia** podemos consultar información pública de cualquier autoridad sin importar su orden, la entidad, o el poder al cual represente, facilitándonos el acceso a la información de nuestro interés sin recurrir a sistemas dispersos.

II. Derecho a la Protección de Datos Personales (DPDP)

Cómo ejercerlo y qué instancias lo protegen



Ahora conoceremos qué es y cómo podemos ejercer **nuestro derecho a la protección de datos personales en posesión de los particulares (DPDP)**, con el objetivo de saber cómo exigir su correcto tratamiento y que garantice nuestra privacidad; o, en otras palabras, **decidir el trato que queremos dar a nuestra información.**

Primero necesitamos saber los **datos personales se refieren a cualquier información sobre una persona física identificada o identificable.** Por otra lado, existen los **datos sensibles** que son también nuestra información personal, pero se refieren a una **esfera más íntima de nuestras vidas** (incluso, un uso indebido de nuestros datos sensibles puede generar situaciones de discriminación o de riesgo grave).



Todos los datos sensibles forman parte de los datos personales, pero no todos los datos personales son datos sensibles.

Ahora que sabemos cuáles son nuestros datos personales, a continuación te presentamos quiénes son parte del tratamiento de tus datos y en qué consiste.

SUJETOS EN LA PROTECCIÓN DE DATOS PERSONALES



TITULAR

Es la persona física a quien refieren y pertenecen los datos personales. Es decir, es el dueño de los datos personales.

Ejemplo: un trabajador del cual se integra un expediente laboral.



RESPONSABLE

Es la persona física o moral privada que establece las finalidades del tratamiento o el uso que se le dará a los datos personales.

Ejemplo: la empresa que contrata al trabajador e integra su expediente laboral.



ENCARGADO

Es la persona física o moral, ajena a la organización del responsable del tratamiento, que trata los datos personales a nombre y por cuenta del responsable.

Ejemplo: la empresa contratada por el responsable para administrar su nómina.

Fuente: Elaboración propia.




TRATAMIENTO DE DATOS PERSONALES



Fuente: Elaboración propia.

Saber esto nos permite estar plenamente conscientes de los principios y entes involucrados en la protección y el tratamiento de nuestros datos personales, lo cual es de gran importancia considerando que es muy común que diversas personas físicas o morales, intenten recabar nuestra información para diversos fines. Por ejemplo, las casas encuestadoras que desean conocer nuestra opinión o preferencias sobre ciertos temas, empresas que necesitan nuestros datos para proveernos de un bien o servicio, como las de telefonía móvil o las televisión de paga, o en las que buscamos empleo.

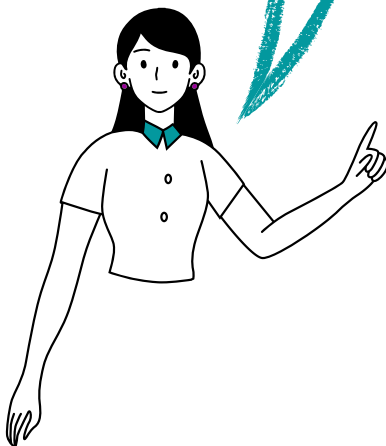
¿CÓMO PUEDEN OBTENER MIS DATOS PERSONALES?



DE FORMA PERSONAL	Quando el titular proporciona sus datos personales al responsable con la presencia física de ambos.	Ejemplo: cuando el titular acude a un consultorio médico.
DE FORMA DIRECTA	Quando el titular proporciona sus datos personales a través de un medio (electrónico, óptico, sonoro, visual, etc.) que permita su entrega directa al responsable.	Ejemplo: cuando llenamos un formulario en internet o hacemos llegar nuestros datos por correo electrónico.
DE FORMA INDIRECTA	Quando el responsable obtiene los datos personales sin que el titular se los haya otorgado de forma directa o personal.	Ejemplo: a través de transferencias o fuentes de acceso público.

Fuente: Elaboración propia.


Parece un poco arriesgado confiar nuestros datos personales a otras personas, pero recuerda que la ley obliga a que los responsables de su obtención y tratamiento a actuar responsablemente, y a cumplir una serie de principios.



PRINCIPIOS Y DEBERES PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES


LICITUD

Solo se podrá hacer con los datos personales aquello que esté permitido por las leyes en general y en la normatividad sobre protección de datos personales en particular.




LEALTAD

La obtención de nuestros datos personales no podrá hacerse a través de medios engañosos ni fraudulentos, respetando la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado en el aviso de privacidad.




CONSENTIMIENTO

El responsable debe contar siempre con el consentimiento tácito, expreso para el tratamiento de nuestros datos especificando las finalidades que persigue. Asimismo, deben informarnos los cambios en las finalidades del aviso de privacidad para obtener nuevamente su consentimiento.




FINALIDAD

Los responsables deberán especificar para qué objeto se tratarán nuestros datos personales de manera clara, sin lugar a confusión y con objetividad. Esto implica que se deben evitar finalidades inexactas, vagas o ambiguas.




INFORMACIÓN

Los responsables se encuentran obligados a darnos a conocer las características principales del tratamiento de nuestra información personal, a través de un aviso de privacidad que sea sencillo, cuente con información necesaria, use un lenguaje claro y comprensible.




CALIDAD

Conforme las finalidades para las que se vayan a tratar nuestros datos personales, estos deben ser: exactos, completos, pertinentes, correctos y estar actualizados a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicho supuesto.




PROPORCIONALIDAD

Es obligación del responsable tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron. Asimismo, implica que el responsable debe realizar los esfuerzos para que los datos tratados sean los mínimos necesarios para lograr las finalidades para las cuales se obtuvieron.



RESPONSABILIDAD

Los responsables se encuentran obligados a darnos a conocer las características principales del tratamiento al que será sometida la información personal, lo que se materializa en la elaboración y puesta a disposición del aviso de privacidad que sea sencillo, cuente con información necesaria, use un lenguaje claro y comprensible, y que su estructura y diseño sean de fácil entendimiento.



Fuente: INAI, Guía para cumplir con los principios y deberes de la Ley Federal para la Protección de Datos Personales en Posesión de Particulares, México, 2014, pp. 15-68.

RESPONSABILIDADES DE ENTES QUE POSEAN NUESTROS DATOS PERSONALES

Confidencialidad

Implica la obligación de guardar secreto respecto de los datos personales que son tratados con el objetivo de evitar causar daño a su titular. Para ello, el responsable tiene que adoptar medidas para evitar que quienes tengan acceso a los datos personales divulguen dicha información o para evitar que un tercero no autorizado pueda tener acceso a los mismos.



Seguridad

Se refiere a la obligación de establecer y mantener medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Las medidas de seguridad, pueden ser técnicas, físicas y administrativas, y deben prevenir vulneraciones tales como pérdida o destrucción de bases de datos, su robo, extravío o copia, el uso no autorizado, acceso o tratamiento de datos personales.

Fuente: Elaboración propia.

Además de los principios enunciados anteriormente, quienes manejan nuestros datos personales tienen otras responsabilidades, importante como las de confidencialidad y de seguridad al tratar nuestros datos personales.



Todos estos deberes y principios se traducen en la **expectativa razonable de privacidad**, esto significa que **depositamos cierta confianza con respecto al uso que se le darán a nuestros datos personales conforme a lo acordado con quien recibe dicha información y lo que marca la Ley**, lo cual podemos constatar a través del **aviso de privacidad**.

Asimismo, siendo **información personal**, el tratamiento de nuestros datos **está sujeto a nuestro consentimiento explícito**, ya sea de forma verbal, escrita, por medios electrónicos, ópticos, entre otros.

AVISO DE PRIVACIDAD

1 Documento físico, electrónico o en cualquier otro formato que el responsable en el tratamiento de los datos personales pone a disposición del titular.

4 Debe contener identidad y domicilio de quien recaba los datos, opciones y medios para que los titulares limiten el uso o divulgación de los mismos

2 A través de este, se le comunica al titular los datos personales que se recabarán y los fines para los cuales se hará.

3 También debe contener los medios para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición.

Fuente: Elaboración propia.

Confiar nuestros datos personales no quiere decir que los entregamos y no podemos hacer nada. ¡Al lo contrario! **Podemos revocar o retirar nuestro consentimiento para el tratamiento de nuestros datos personales** a través de un procedimiento gratuito y más sencillo que el que se utiliza para obtener tu consentimiento. Es decir, el ente **responsable debe ofrecerte las mismas facilidades para revocar tu consentimiento, que para obtenerlo.**

En ocasiones, por desinterés, apuro, desconocimiento u otras razones, no damos importancia al uso que los particulares pueden hacer de nuestros datos personales, o nos parece irrelevante que exista un aviso de privacidad al final de las formas que llenamos en físico o en internet, pero es muy importante que lo revisemos.

Es importante poner atención en el aviso de privacidad pues si no manifestamos oposición a un aviso que se puso a nuestra disposición, damos nuestro consentimiento para el uso de nuestros datos personales



Como titulares de datos personales, podemos ejercer nuestro derecho a la protección de datos personales mediante al acceso, rectificación y cancelación, así como a manifestar su oposición a su tratamiento, lo que se conoce como **derechos ARCO.**

Podemos **ejercer nuestros derechos ARCO**, únicamente necesitamos **solicitarlos ante el INAI o ante el responsable del tratamiento de nuestra información**, acreditando que somos los titulares de los datos personales, presentando nuestro nombre, domicilio, acreditar nuestra identidad y describiendo los datos personales sobre los cuales buscamos ejercer estos derechos.

DERECHOS ARCO

A

ACCESO

A partir de este derecho podemos conocer cuál es la información personal que está en posesión del responsable, el estado en que se encuentra (es decir, si es correcta y actualizada), los fines para los cuales se utiliza; así como las características generales del uso al que están sometidos nuestros datos personales.

R

RECTIFICACIÓN

Este derecho nos permite rectificar nuestra información personal cuando esta sea incompleta o inexacta; es decir, podemos solicitar al responsable que corrija nuestros datos de ser erróneos, desactualizados o inexactos.

C

CANCELACIÓN

Gracias a este derecho podemos solicitar que se eliminen nuestros datos personales cuando consideremos que su tratamiento no se está llevando a cabo conforme a las obligaciones que tiene el responsable de acuerdo a la Ley.

O

OPOSICIÓN

Tenemos el derecho de oponernos al uso de nuestra información personal o exigir el cese del mismo cuando, por alguna causa legítima, sea necesario parar el uso de nuestros datos personales para evitarnos algún daño, o cuando no queremos que sean utilizados para ciertos fines o por ciertas personas.

Fuente: INAI, Guía para cumplir con los principios y deberes de la Ley Federal para la Protección de Datos Personales en Posesión de Particulares, México, 2014, pp. 8-9.

Para ejercer nuestros derechos ARCO, en primera instancia, debemos presentar de forma gratuita, una solicitud ante el ente responsable del tratamiento de nuestros datos personales, el cual debe contar con una persona o departamento de datos personales, encargada de dar trámite a las solicitudes de ejercicio de estos derechos.

ELEMENTOS PARA LA SOLICITUD DE DERECHOS ARCO



El nombre del titular de los datos personales, domicilio u otro medio para comunicarle la respuesta a su solicitud.



Los documentos que acreditan nuestra identidad.



La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO.

Fuente: Elaboración propia.

Una vez que presentamos nuestra solicitud para el ejercicio de nuestros derechos ARCO, el responsable tiene un plazo máximo de 20 días hábiles para determinar e informarnos si esta procede o no. Como en las solicitudes de acceso a la información, dicho plazo puede extenderse por un periodo similar siempre que el ente responsable en el tratamiento de nuestros datos personales, lo justifique y lo haga de nuestro conocimiento.

Sin embargo, en ocasiones, el responsable puede negarse al ejercicio de los derechos ARCO.



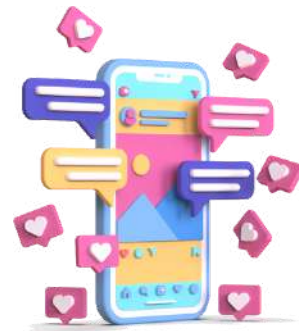
A pesar de que el responsable en el tratamiento de nuestros datos personales nos niegue el acceso, rectificación, cancelación u oposición, debe darnos una respuesta en la que nos informe los motivos de su negativa.

También es importante saber, **que en caso de que no se haya atendido nuestra solicitud de derechos ARCO**, o de no estar conforme con la respuesta otorgada por el responsable, **podemos acudir al INAI para presentar una inconformidad** a través del procedimiento de protección de derechos, a fin de que **el Instituto resuelva si procede o no la respuesta que te fue otorgada, o requiera al responsable que atienda tu solicitud de ejercicio de derechos ARCO.**

podemos acudir al INAI para denunciar un uso indebido de nuestros datos personales. **El procedimiento es similar a una solicitud de protección de derechos, por lo que debemos señalar nuestro nombre y domicilio, la relación de los hechos en los que basamos nuestra denuncia** y los elementos con los que contamos para probar lo dicho, así como el nombre y domicilio de quien denunciarnos. Una vez recibida la denuncia, el INAI la valorará e iniciará un proceso de verificación el cual tiene una duración máxima de 180 días hábiles, y que culmina con la resolución del Instituto en la que se determina si el responsable incumplió con la Ley, en cuyo caso, se establecerán las medidas que deberá adoptar el responsable, así como las sanciones que pueden ser aplicables en su contra.



III. Cuido mi información en redes sociales

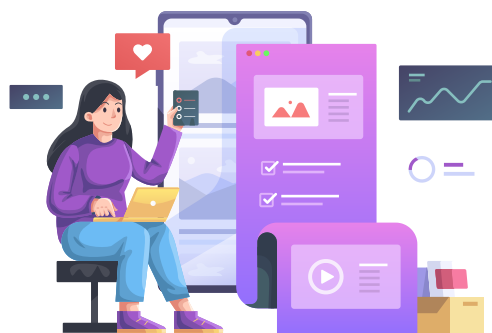


Las **redes sociales** son el principal medio de comunicación y canal para la expresión entre la población joven y han sido una grandiosa herramienta para difundir talentos y defender causas, además de conectar a las personas a pesar de la distancia.

Las redes sociales también son entretenidas y ahí encontramos memes muy divertidos, muchos videos de gatitos y perritos. Sin embargo, el uso incorrecto puede provocar situaciones de riesgo.



En la actualidad, la mayor parte de las personas con acceso a internet tiene al menos una red social, a través de la cual, con apoyo de nuestros dispositivos, es común compartir información sobre nuestra identidad, dirección y ubicación.



Esta práctica es muy común, pero no es inofensiva y ponen en riesgo nuestra seguridad y la de quienes nos rodean.

Vamos a revisar cómo sucede y cómo podemos evitarlo.

La información que compartimos a través de redes sociales nos expone al robo de información, a través de estas plataformas es posible la suplantación de identidad (cuando otra persona se hace pasar por ti utilizando tus datos e incluso fotografías), el acoso o ciberbullying (cuando una personas investiga todos tus movimientos y/o te escribe mensajes negativos de forma constante), y el robo de cuentas personales, por mencionar algunos de los riesgos.

Actividades que pueden provocar riesgos en redes sociales

- 

Publicar la ubicación en tiempo real en redes sociales
- 

Compartir fotografías o videos de viajes
- 

Dar a conocer el domicilio particular, ya que, a través de esta información, se abre la posibilidad de que los delincuentes localicen a los usuarios, planeen y ejecuten robos a casa habitación, entre otros
- 

Compartir contraseñas o utilizar las mismas contraseñas para todas las redes

De acuerdo con la ONU, **las redes sociales son el mecanismo más recurrente para reclutar víctimas** (UNODC, 2020), además de que en ellas también se presentan otras situaciones como el grooming, ciberbullying, phishing, sexting, la usurpación de identidad, el secuestro y la extorsión, ¿sabes qué significan?

Expresiones de violencia digital

CIBERBULLYING

Es el que se lleva a cabo a través del uso de medios de comunicación, principalmente de redes sociales y videojuegos online para cometer acoso psicológico.



PHISHING

es una forma de delincuencia por la cual una persona suplanta a una entidad o institución con el fin de obtener información o datos de confidencialidad de sus víctimas, tales como claves de tarjetas, contraseñas de redes sociales, códigos de seguridad o dígitos de seguridad de tarjetas de crédito, entre otras.



CIBERFLASHING

es la práctica de enviar fotos íntimas a una persona sin su consentimiento. En la mayoría de los casos, se trata de hombres que hostigan a mujeres con imágenes de sus genitales.



SEXTING

Consiste en enviar mensajes, fotografías o videos de carácter sexual a través de Internet, siendo la mensajería instantánea y las redes sociales los canales más utilizados.

El principal problema del sexting es la difusión, cuando una imagen sale de un teléfono móvil, se pierde control de ella.



STALKED

Son aquellas conductas que realiza una persona conocida como *stalker*, consistentes en perseguir, acechar y acosar, mediante plataformas tecnológicas de forma compulsiva a otra persona.



SEXTORSIÓN

Aunque puede llegar a estar muy relacionado, cabe no confundir este término con el sexting. La sextorsión se trata de chantaje sexual. El extorsionador chantajea a la víctima con contenido privado del usuario, normalmente fotos o videos sexualmente explícitos.



GROOMING

Es el acoso ejercido por una persona adulta hacia un (a) niño/a o adolescente con el propósito de establecer una relación de control emocional y de abuso sexual.



SHAMING

Últimamente se han empleado los términos fat-shaming y slut-shaming para nombrar aquellos actos que tienen el objetivo de avergonzar a la víctima. El primer término se refiere a la complexión física y el segundo a comportamientos y deseos sexuales.



DOXING

Consiste en la acción de publicar información privada sin consentimiento de la persona.



Debemos ser cuidadosos acerca de la información que compartimos a través de internet debido a que no hay posibilidad de ser borrados definitivamente.

Por esto, debemos tomar la responsabilidad de nuestra información y cuidarla con mucha atención, ya que nuestros datos personales poseen un gran valor.



A continuación te sugerimos algunas actividades sobre cómo proteger tu información y datos personales en Internet:

¿CÓMO CUIDAR MIS DATOS E INFORMACIÓN PERSONAL?

Rechaza a cualquier persona desconocida que quiera contactarte en la web. Evita agregar o contactar a usuarios desconocidos o con los que no se tenga relación alguna, además sólo abre y contesta correos electrónicos de la gente que conozcas.

Utiliza un perfil de redes privado o en caso de que sea público, agregar restricciones de quién puede ver lo que publicas.

Asegurate de cerrar adecuadamente tu sesión al ingresar a las redes sociales desde cibercafés y computadoras públicas o compartidas.

Procurar no hacer transacciones comerciales en redes sociales o en sitios web que se desprendan de éstas.

Activa la verificación de dos pasos de tus redes.

Revisa la política de privacidad de los sitios de internet a los que proporcionas datos.

Difunde tu información personal de manera controlada, consciente y responsable, ya que una vez cargada a una plataforma, será pública y de fácil acceso.

Fomenta en tu entorno familiar y social, el uso responsable de datos personales en las redes sociales y/o al navegar en Internet.

Nunca compartas tus contraseñas o claves de acceso a otras personas y cámbialas con frecuencia. En internet puedes encontrar diversas paginas que te ayudarán a generar contraseñas.

No realices compras en internet sin la supervisión de tus padres.

The infographic features several icons: a person with a key, a shopping cart, a smartphone, a padlock, a person with a magnifying glass, and a group of people. The background is a light blue and yellow gradient.

¿Cómo cuido mis contraseñas? Ejercicio

A continuación, te proponemos palomear aquellas características con las que cuentan tus contraseñas para que puedas conocer su nivel de seguridad:

-Usas contraseñas distintas para múltiples cuentas, especialmente si estas son importantes.

-Usas una clave que tenga como mínimo las siguientes características: 16 caracteres, un número, una letra mayúscula, una letra minúscula, y un símbolo especial.

-No usas los nombres y apellidos de tu familia, amigos o mascotas como tus contraseñas.

-En tus contraseñas no incluyes cumpleaños, códigos postales, números de casas, números de teléfono, etc.

Guía para configuración de privacidad de redes sociales

Una medida muy importante para proteger tus datos es configurar correctamente la privacidad de tus redes sociales y aplicaciones de mensajería. A continuación, se presentan los pasos para configurar la privacidad de las principales redes sociales:





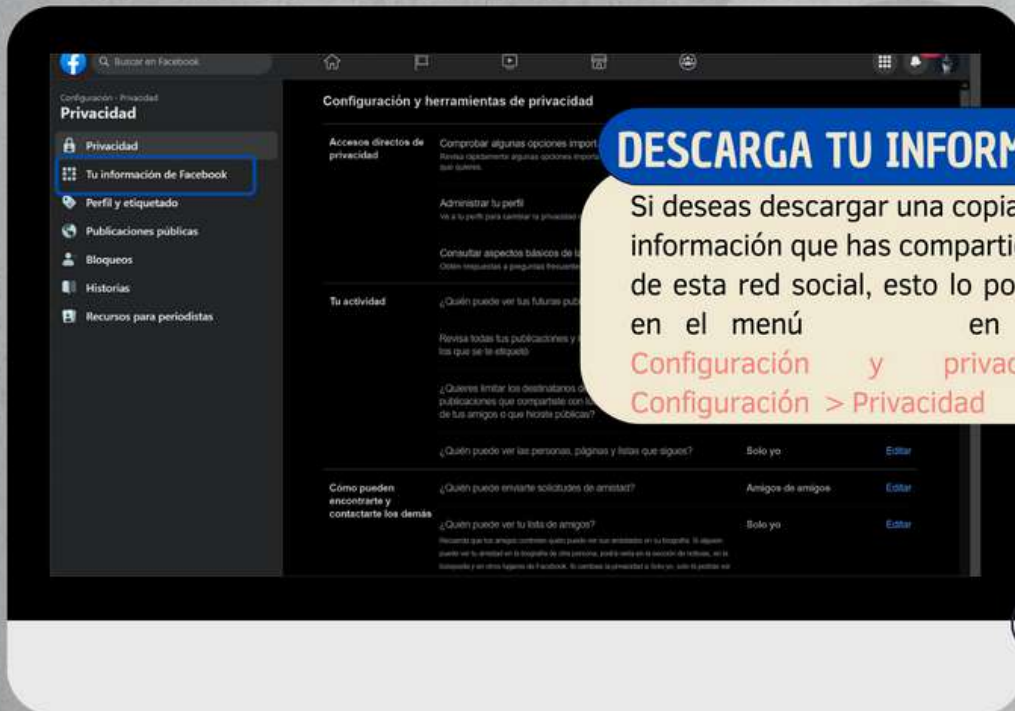
COMPROBACIÓN RÁPIDA DE SEGURIDAD

Realiza una revisión rápida de privacidad, a través del menú **Configuración y Privacidad > Comprobación rápida de privacidad** donde se revisarán las configuraciones de privacidad de las publicaciones, la información de perfil y las aplicaciones y sitios web en los que iniciaste sesión con Facebook.



DESCARGA TU INFORMACIÓN

Si deseas descargar una copia de toda la información que has compartido a través de esta red social, esto lo podrás hacer en el menú **Configuración y privacidad > Configuración > Privacidad**





CONFIGURACIÓN Y HERRAMIENTAS DE PRIVACIDAD

Para configurar la actividad en el perfil, así como las personas que pueden ponerse en contacto contigo, en el menú consulta el apartado **Configuración y privacidad > Configuración > Privacidad**



APLICACIONES Y SITIOS WEB

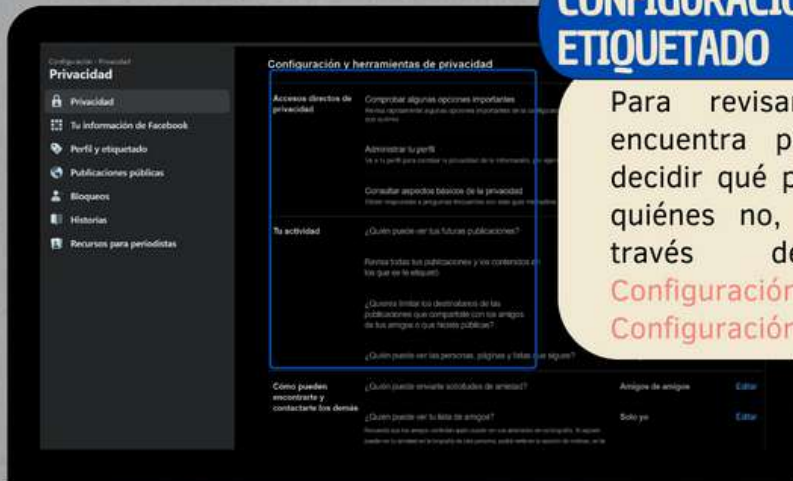
Si quieres controlar el acceso y los permisos que aplicaciones de terceros, sitios web y juegos tiene a tu información personal debes ingresar al menú **Configuración y privacidad > Configuración > Seguridad e inicio de sesión > Apps y sitios web**

Por cada una de ellas se podrá configurar el acceso a datos, la información que se proporciona a la aplicación para su funcionamiento, quién puede ver que se usa la aplicación, los permisos sobre el envío de notificaciones, los medios para conocer la política de privacidad de la aplicación, la información para eliminar los datos recopilados por la aplicación y los datos de ayuda de los desarrolladores.

Asimismo, en esta sección puedes editar las preferencias sobre el intercambio de datos, desactivando de manera general los accesos a aplicaciones, sitios web y juegos, las notificaciones de juegos y aplicaciones y controlando la privacidad de aplicaciones que utilizan versiones antiguas de Facebook para celulares.

CONFIGURACIÓN DE BIOGRAFÍA Y ETIQUETADO

Para revisar qué información se encuentra pública en tu perfil y decidir qué personas pueden verla y quiénes no, puedes configurarlo a través del menú opción **Configuración y privacidad > Configuración > Privacidad**



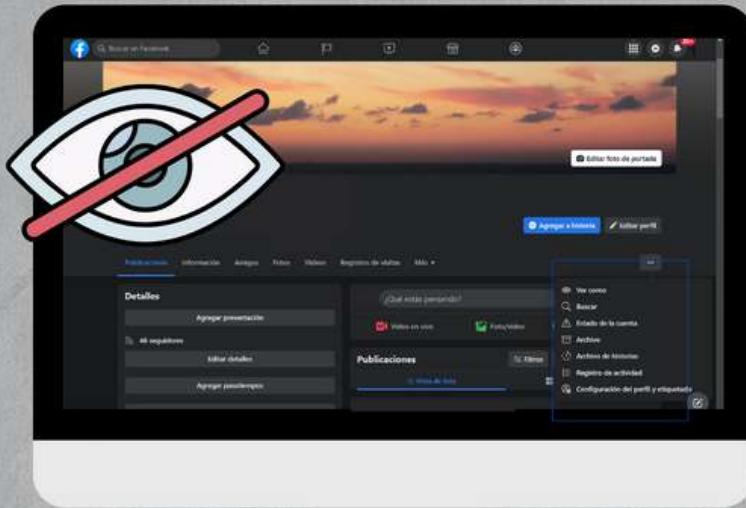
En esta sección también puedes configurar los permisos para el etiquetado de fotografías y/o publicaciones que tus amigos realizan desde su perfil.



De forma específica, para cada publicación que realices, podrás seleccionar quién puede verla a través de una lista de opciones (público, amigos, amigos excepto, amigos concretos, solo yo o personalizado)

VER COMO

verifica periódicamente qué información se encuentra pública en tu perfil, de tal forma que puedas proteger aquella que no deseas que sea vista por personas no autorizadas. Para ello existe la opción **Ver como** que se encuentra disponible dentro del perfil en el menú.



AUTENTICACIÓN EN DOS PASOS

La autenticación en dos pasos es una función de seguridad que, junto a la contraseña, ayuda a proteger tu cuenta de Facebook. Si configuras esta función, se te pedirá que ingreses un código de inicio de sesión especial o que confirmes el intento de inicio de sesión cada vez que alguien intente acceder a Facebook desde un navegador o un dispositivo móvil no reconocido.

Puedes habilitar esta protección ingresando al menú **Configuración y privacidad > Configuración > Privacidad > Seguridad e Inicio de Sesión**.





CONFIGURACIÓN DE PRIVACIDAD Y SEGURIDAD DEL PERFIL

Mediante el apartado **Editar Perfil** podrás configurar la privacidad y seguridad de tu perfil de Instagram.

En esta sección podrás modificar:

Aspectos sobre la privacidad de tu cuenta, las cuales solo están disponibles para las personas que tu apruebes.

Estado de actividad, que permite que las cuentas que sigues y las personas a las que has enviado mensajes puedan ver la última vez que has estado activo en las aplicaciones de Instagram

Compartir historias, permitiendo que las personas compartan tus historias como mensajes

Establecer filtros para los comentarios, añadiendo palabras o frases para que los comentarios que incluyan las palabras que añadiste en la configuración no aparezcan en tus publicaciones.



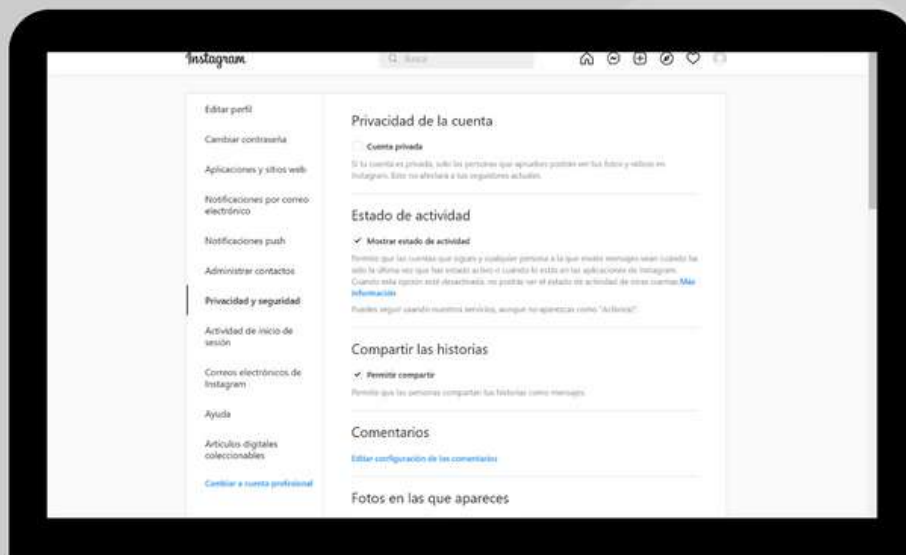


Configurar si quieres añadir automáticamente a tu perfil las fotos en las que apareces cargadas a la aplicación por uno de tus amigos

Configurar datos de tu cuenta, como información general de la cuenta, contactos, información del perfil, actividad

Habilitar la autenticación de dos pasos, donde se te enviará un código de seguridad cada que inicies sesión

Descargar los datos asociados a la cuenta, donde podrás solicitar as fotografías, comentarios, información del perfil y otros datos asociados a tu perfil, información que te será enviada vía correo electrónico



**NEW
POST**



WhatsApp



PRIVACIDAD Y SEGURIDAD



A través del icono de Configuración de la aplicación podrás ingresar al menú Cuenta donde podrás realizar la configuración de privacidad y seguridad de la aplicación.

En sistema operativo APPLE

Da clic directamente en el icono Configuración ubicado en la esquina inferior derecha de tu pantalla.

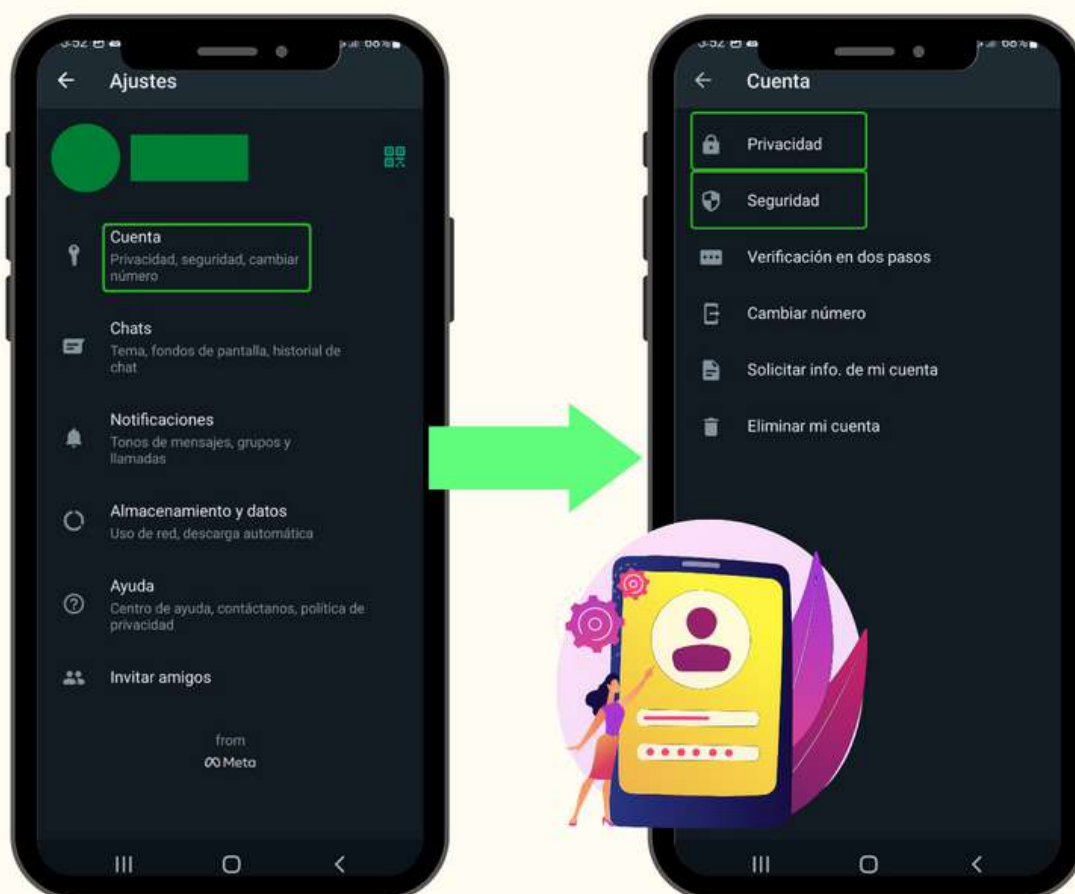


En sistema operativo Android



Da clic primero en el icono  ubicado en la esquina superior derecha de tu pantalla,

después da clic en la opción Configuración.



Si accedes desde la opción Configuración, las opciones de acceso para cada apartado para sistemas operativos Apple y Android son iguales en las opciones que se indican a continuación, por lo que ya no se agrega la imagen para Android.



PRIVACIDAD

En este apartado puedes configurar:

- Quién puede ver la última vez que te conectaste en la app
- Tu foto de perfil
- Información de tu estado
- Ubicación en tiempo real
- La lista de contactos bloqueados
- Habilitar o deshabilitar las confirmaciones de lectura

SEGURIDAD



En este apartado puedes habilitar las notificaciones de seguridad. Esta opción únicamente te notifica cuando el código de seguridad de un contacto cambia.



El cifrado de extremo a extremo en WhatsApp asegura que solo tú y el receptor puedan leer lo que se envía, y que nadie más, ni siquiera WhatsApp, lo pueda hacer.

Tus mensajes se aseguran con candados y solo tú y el receptor cuentan con los códigos/llaves especiales para abrir y leer los mensajes.





VERIFICACIÓN EN 2 PASOS

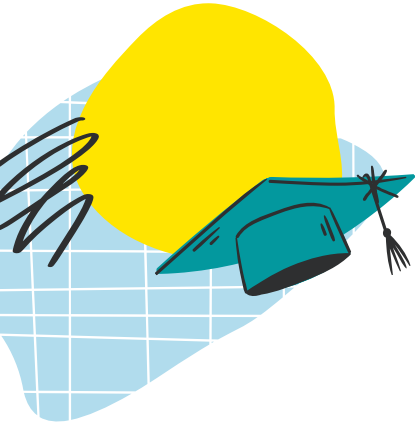
En el menú Verificación en dos pasos podrás activar la verificación a través de un PIN que se solicitará cuando vuelvas a registrar tu número de teléfono en WhatsApp.

SOLICITAR INFORMACIÓN DE MI CUENTA

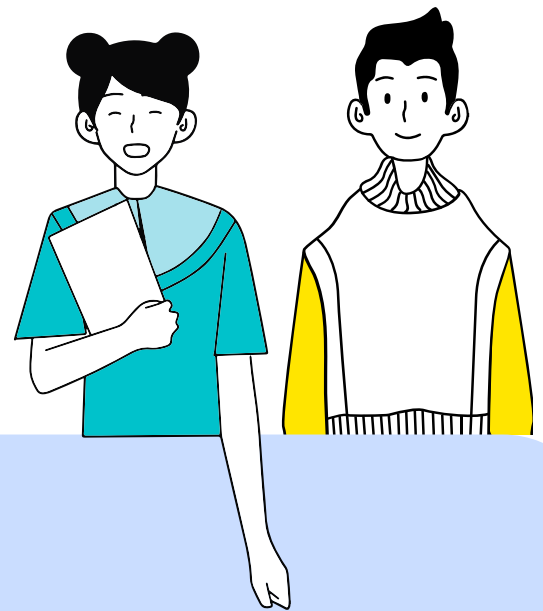
Si deseas solicitar un informe de los ajustes de configuración y de la información de tu cuenta de WhatsApp, puedes hacerlo a través del menú Solicitar info. de mi cuenta en la opción Solicitar Informe



GRACIAS POR PARTICIPAR



No olvides
responder los
cuestionarios y
descargar tu
constancia



ACEDacMX



ACED.AC.MX



ACED AC

Conoce más en:
<https://aced.org.mx/>

