Seguridad de la Información

GUÍA DIDÁCTICA

ANEP Educación Pública

CERTuy Centro Nacional de Respuesta a Incidentes de Seguridad Informática

agesic Desarrollando el Uruguay Digital

Presidencia República Oriental del Uruguay

Seguridad de la Información

GUÍA DIDÁCTICA

Contenidos

Introducción

¿Qué es Seguro te Conectás?

Seguro te Conectás es una campaña de difusión orientada a sensibilizar a los usuarios de internet y dispositivos digitales.

Su objetivo es dar a conocer y aumentar la comprensión de las amenazas informáticas, propiciando un vínculo responsable entre las personas e internet.

La campaña te permitirá informarte acerca de lo que puede afectar tu seguridad en el mundo digital y de qué manera protegerte.

¿Por qué hablar de seguridad de la información?

Niños, jóvenes, adultos se ven desafiados permanentemente ante el uso de las nuevas tecnologías, que facilitan las formas de relacionamiento entre las personas. No obstante, es necesario conocer los riesgos inherentes a esas herramientas y minimizar esos peligros mediante la adopción de conductas seguras.

Para poder pensar en términos de seguridad de la información, es necesario reflexionar acerca de ciertos aspectos importantes: ¿existe información sensible que resulta preciso proteger?, ¿qué consecuencias tendría perder toda esa información?, ¿qué amenazas existen hoy en día que pongan en riesgo la información?, ¿y qué se debe hacer en caso de que ocurra algún problema de vulnerabilidad de la información?

¿Cuál es el objetivo de la guía?

El propósito de esta guía es brindar la información necesaria para desarrollar y fortalecer las capacidades personales que lleven a un uso seguro y confiado de las tecnologías de la información desde múltiples dispositivos y con diversos fines.

Además, generar las bases de conocimiento en seguridad de la información para poder transmitir a terceros las buenas prácticas en el tema y así generar una cultura más segura.

¿Qué contiene y a quién está dirigida?

Esta guía desarrolla los aspectos más relevantes en materia de seguridad de la información que afectan nuestra vida cotidiana. En ella se abordan temas como la importancia de proteger la información, tener contraseñas seguras, hacer copias de seguridad, evitar el spam, consejos para comprar en línea, cómo reconocer páginas seguras y cómo manejar la privacidad en redes sociales, entre otros.

La guía está organizada en cinco unidades, en cada una de las cuales se desarrollan contenidos temáticos y se proponen actividades didácticas.

El documento está dirigido a docentes, educadores y público en general.

1

El valor de la información

Temas a abordar:

- Sensibilizar acerca del valor que tiene la información y cómo protegerla.
- Destacar la importancia de clasificar la información y tratarla adecuadamente.
- Promover el cuidado y la protección de la privacidad de la información.

Introducción

Las personas manejan y generan a diario mucha información: lo que escriben, lo que hablan y lo que hacen en los distintos ámbitos de sus vidas contiene información, la cual tiene un valor determinado por cada persona. Por esta razón, es importante proteger y gestionar de forma segura toda esa información, tales como los contactos telefónicos, los amigos en redes sociales, las fotos, los documentos que se firman, los videos que se crean y las conversaciones que se mantienen.

El valor de la información

"Proteger la información" no significa ocultarla, sino tratarla conforme al valor que tiene para cada persona. Esto implica no solo proteger la información propia, sino también manejar con responsabilidad la información de terceros.

¿Esa selfie es pública?

ASEGURATE

Antes de publicarla, asegurate que a esa foto solo la pueden ver tus amigos. Evitá una exposición no deseada o que alguien pueda usar tus imágenes para perjudicarte.

Buena parte de la información que manejamos a diario contiene **datos personales.**

Un **dato personal** es cualquier tipo de información que pueda identificar directamente o haga identificable a una persona, ya sea su nombre, dirección, teléfono, cédula de identidad, RUT, imagen, huella digital, número de socio, número de estudiante o hasta el ADN.

Los **datos sensibles** son aquellos datos personales que revelan el origen racial o étnico, las preferencias políticas, las convicciones religiosas o morales, la afiliación sindical o la vida sexual de una persona. Estos datos se consideran sensibles ya que requieren mayores grados de protección y su divulgación inadecuada podría generar un perjuicio para su titular. Para recolectar y tratar este tipo de datos se requiere el consentimiento expreso y escrito del titular, salvo algunas excepciones establecidas por la Ley N° 18.331.

También hay otro tipo de datos que por sus características están especialmente protegidos:

Los **datos relativos a la salud**. Son aquellos tratados por instituciones y profesionales de la salud, quienes deben guardar el secreto profesional y manejarlos de acuerdo a la legislación sanitaria y la Ley N° 18.331.

Los **datos relativos a las telecomunicaciones**. Las personas físicas o jurídicas, públicas o privadas, que actúan en el ámbito de las telecomunicaciones deben garantizar la protección de los datos personales y cumplir con las exigencias legales.

Los **datos relativos a bases de datos con fines publicitarios**. Son aquellos datos que permiten establecer un perfil de consumidor para fines promocionales, comerciales o publicitarios.

Los **datos relativos a la actividad comercial o crediticia**. Cuando es necesario conocer la solvencia patrimonial o crediticia, la ley establece determinadas condiciones para manejar esta información dentro de los marcos de privacidad establecidos.

En nuestro país, la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data del 11 de agosto de 2008 regula la protección de los datos personales y establece derechos y obligaciones al respecto.

¿Cómo proteger la información?

Si se decide que no se quiere compartir con cualquier persona determinada información, entonces se debe definir el **nivel de privacidad** que corresponde atribuirle, clasificándola según determinados criterios.

La información puede ser clasificada y tratada de forma diferenciada para darle los niveles de seguridad que se desea. Para hacerlo, cuando se envía o se publica información es necesario analizar y evaluar en primer término qué se desea transmitir, con qué finalidad, a quién está dirigida, cuál es el lenguaje más adecuado para transmitirla, qué medio se utilizará y en qué ámbito o contexto será utilizada.

Contenido del mensaje: determinar qué información se quiere transmitir.

Clasificar la información: decidir el grado de privacidad que requiere.

Elegir cómo y dónde transmitirla: correo electrónico, redes sociales, otros.

Verificar las medidas de seguridad correspondientes.

Aspectos a tener en cuenta

Definir el contenido del mensaje: Implica ser conscientes de qué información deseamos transmitir, si realmente es necesario hacerlo y qué información será incluida en lo que enviaremos o publicaremos.

Clasificar la información: Una vez determinada la información, deberemos analizarla de acuerdo al valor que tiene para nosotros y el grado de sensibilidad preguntándonos a quiénes debería dirigirse y también quiénes no deseamos que accedan a ella. Esto determinará el grado de privacidad adecuado y el ámbito en el cual la divulgaremos.

Elegir cómo y dónde transmitir la información: De acuerdo al ámbito o grupo de personas a las cuales dirigiremos la información, deberemos seleccionar por qué medio la transmitiremos para cumplir con los criterios que establecimos en el paso anterior.

Verificar las medidas de seguridad pertinentes: Cuando compartimos información por cualquier medio, debemos verificar que efectivamente lo estamos haciendo de manera correcta, dentro del marco de privacidad que decidimos darle. Por ejemplo: si deseamos compartir una foto en Facebook solo con nuestros amigos, debemos verificar su nivel de privacidad antes de publicarla.

Ámbitos de circulación de la información

De acuerdo al valor que se le atribuye a la información (propia y de terceros) que se desea transmitir, se puede seleccionar el ámbito en el cual habrá de circular:

Público. La información es accesible a todo público: en internet, en la calle, en las redes sociales, en el ómnibus, en el ascensor, en restaurantes, en comercios, etc.

Social. La información se comparte o se socializa en un grupo específico de personas; por ejemplo: compañeros de estudio, club deportivo, vecinos, etc.

Laboral. La información relacionada a nuestro trabajo y a la organización laboral en la que nos desempeñamos se comparte en forma restringida a ese ámbito y de acuerdo con las normas que generalmente cada una establece al respecto.

Amigos. Compartimos información con determinado círculo de personas allegadas, pudiendo tener más de un grupo de amigos según diferentes grados de confianza o conocimiento.

Familiar. Es un ámbito de relaciones familiares en el que manejamos y compartimos información propia, de padres, hijos, hermanos, etc.

Íntimo. Se trata de un ámbito en el cual se decide no compartir información con nadie o hacerlo con una o muy pocas personas que merecen extrema confianza.

Casos para analizar y reflexionar

Caso 1: Susana en el trabajo

Situación

Susana decide sacarse una *selfie* en su trabajo y publicarla en una red social.

Consigna de trabajo

Identificá qué información está divulgando y respondé esta pregunta: ¿Qué consecuencias no deseadas podría tener Susana el hacer pública esa *selfie*?

Pautas para la reflexión

Susana muestra en su *selfie* una serie de informaciones, como por ejemplo, ... Esto implica riesgos para ella, pues esa información podría terminar en malas manos. Generalmente, las personas no toman conciencia de cuánta información se ofrece a través de las redes sociales

Preferencias políticas

Clave de acceso

Susana 1234

Datos de contacto

Nombre:
Juan
Teléfono:
093 000 000
Dirección:
18 de julio 100

Caso 2: Laura de vacaciones

Situación

Laura se va de vacaciones con su familia y realiza una publicación en Facebook solicitando ayuda para cuidar a sus mascotas.

Consigna de trabajo

Identificá qué tipo de información está publicando Laura. ¿Creés que podría existir un riesgo para ella al hacerlo?

Pautas para la reflexión

La casa de Laura estará vacía por varios días. Divulgar la dirección de su casa además de la información de que no estarán a muchos amigos, algunos de los cuales tal vez no conoce, implica un mayor riesgo de robo.

Caso 3: Martín en el cuarto de su amigo

Situación

Martín se saca una *selfie* mientras se encuentra en el dormitorio de un amigo y publica esa foto en las redes sociales.

Consigna de trabajo

Identificá qué información está publicando Martín y ordená los datos de mayor a menor según el nivel de privacidad que te parezca adecuado para cada uno.

Pautas para la reflexión

Cada persona le asigna un valor a su información y tiene el derecho de decidir qué se hace con ella, lo que implica también su responsabilidad en el manejo adecuado de la información perteneciente a otras personas. Por tal motivo, antes de publicar información, se debe analizar la situación y preguntarse cuál es el nivel de seguridad que se debería asignarle y en qué ámbitos es adecuado compartirla.

Para recordar:

- Toda información tiene valor, en especial, los datos personales, que están protegidos por ley.
- Para dar a la información los niveles de privacidad adecuados, es necesario analizarla antes de compartir o publicar.
- Manejá la información propia y ajena con responsabilidad.

2

Gestión de la seguridad de la información

Temas a abordar:

- Identificar y prevenir distintas formas de perder información.
- Aportar herramientas para gestionar la seguridad de la información propia y ajena.
- Brindar recomendaciones útiles para gestionar la seguridad de la información en distintos dispositivos.

Introducción

Sin ser conscientes de ello, se puede poner en riesgo la información personal de distintas formas y por distintos medios.

¿Cómo cuidás tu información personal?

ASEGURATE

Tus datos, la ubicación o tu historial de compras tienen mucho valor. Informate sobre quién obtiene esa información y que el sitio, la aplicación o el dispositivo que la recopile sea seguro.

¿De qué forma se pone en riesgo la información?

Exponiendo documentos privados

Cuando se trata de información que no se quiere hacer pública, ya sea en papel o en formato digital, es fundamental tomar las precauciones para que no quede expuesta; por ejemplo, no dejar documentos en impresoras de uso compartido y no dejar sesiones abiertas en computadoras o dispositivos de uso compartido.

Es responsabilidad de cada persona proteger esa información cuando se trabaja con ella.

Cuando se quiere desechar esa información, es importante destruirla de forma definitiva.

A través de las comunicaciones

Lo que las personas dicen y escriben, así como dónde y cuándo lo hacen, también debe ser objeto de cuidado. Las conversaciones a través del celular, en el ómnibus, en la sala de espera del médico o en la cola de un comercio contienen información de valor para vos o alguien más que puede ser escuchada por otras personas que la divulguen de manera perjudicial para los involucrados.

A través de dispositivos

Hoy en día se puede acceder fácilmente a la información personal: contactos, redes sociales, correo electrónico, desde un dispositivo móvil (celular, tablet, notebook) o una computadora. Por esta razón, es importante protegerlos adecuadamente.

Acciones para utilizar los dispositivos con seguridad

Bloqueo de dispositivos

Respaldo de información

Actualizar configuración de dispositivos y antivirus

Contraseñas seguras

La contraseña es una clave que, asociada a un nombre de usuario, permite acceder a un dispositivo o cuenta. Sin la contraseña, el dispositivo o cuenta resultan inaccesibles. De esta forma, la contraseña permite mantener protegida la información.

Una contraseña se considera segura cuando cumple con estos requisitos:

- Tiene al menos ocho caracteres.
- Combina mayúsculas y minúsculas.
- Contiene caracteres especiales.
- Contiene números.

Una forma fácil de generar una contraseña segura consiste en asociarla a una pregunta sencilla para vos o a una frase que puedas recordar fácilmente, pero que no sea fácilmente reconocible o evidente para otras personas.

Evitá usar una misma contraseña para todo y cambiá tus contraseñas con periodicidad.

Consejos para crear una contraseña segura

En la medida en que el sistema o sitio te lo permita, utilizá contraseñas:

- Con al menos 8 dígitos
- Que combine números, letras y símbolos

Uno de los principios de las contraseñas seguras es que sea fácil de recordar y difícil de adivinar.

A continuación, verás algunas estrategias para que logres crear contraseñas que cumplan esos requisitos.

Estrategia 1: Generá una frase larga

Creá una frase que te resulte familiar.

Ejemplo:

Frase: “La pizza fría me encanta”

Contraseña: **LaPizzaFríaMeEnc@nt@**

Acá se utiliza un mecanismo de generación de contraseñas en el que cada palabra comienza con mayúscula; la última palabra sustituye las vocales por números o símbolos.

Importante:

Para robustecer la estrategia, utilizá frases distintas para los diferentes usos. Por ejemplo, utilizá una frase para redes sociales, otra para el correo, otra para el trabajo, otra para portales a los que accedas esporádicamente, etc.

Estrategia 2: Generá una contraseña a partir de una frase

En línea con la estrategia 1, creá una frase larga que te resulte fácil de recordar.

Ejemplo

Frase: “Todas las mañanas me levanto a la misma hora y como tres galletas”.

Contraseña: **TlmmlalmhyC3G**

Aquí se utiliza un mecanismo propio para la generación de la contraseña, en el cual la contraseña toma la primera letra de cada palabra y comienza y termina siempre con mayúsculas. Recordá incluir algún número y/o símbolo.

Estrategia 3: Utilizá gestores de contraseñas

Los gestores de contraseñas, además de guardarlas, te permiten crear contraseñas fuertes. Ejemplos de gestores: KeePass, Password Safe y los provistos por soluciones antivirus, entre otros.

Bloqueo de dispositivos

Seguramente, no saldrías de tu casa dejando la puerta abierta, ¿verdad? El mismo principio se aplica a los dispositivos que usás. Todos tus dispositivos tienen información valiosa que debe ser protegida.

Es importante bloquear la pantalla del dispositivo cuando terminás de usarlo.

Para mayor seguridad, podés configurar el dispositivo para que se bloquee automáticamente.

Esta configuración es especialmente importante en el caso de los celulares y tablets, ya que son muchas las posibilidades de que los roben o se pierdan. En el caso de las computadoras que se encuentran en espacios compartidos, también existe un riesgo muy alto de que otras personas accedan a tu información.

¿No tenés clave en el celular?

ASEGURATE

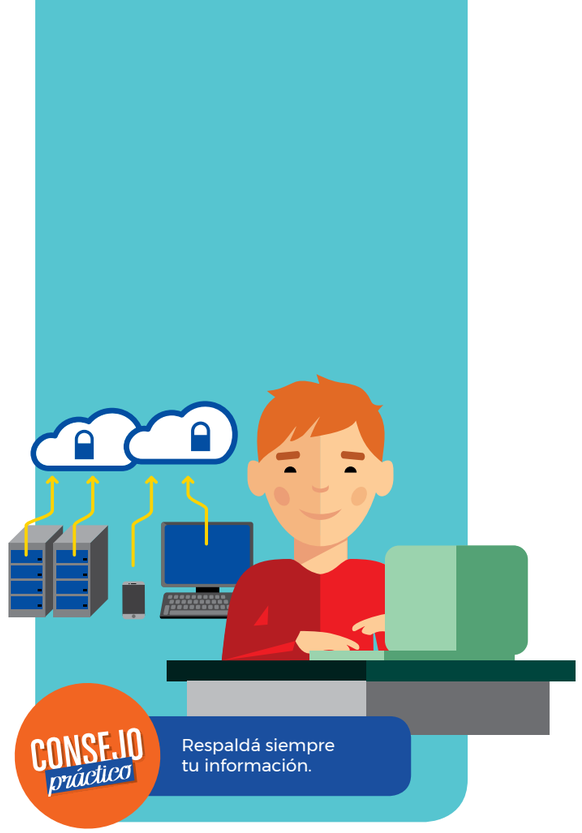
Asegurate siempre de bloquear tu dispositivo con un pin, contraseña o huella digital, así nadie podrá acceder fácilmente a la información que tenés guardada.

Respaldo de la información

Un respaldo es una copia de tu información. Es deseable que tus respaldos no se encuentren almacenados en el mismo dispositivo que contiene tu información. Esto es muy importante debido a que existen múltiples causas por las cuales un usuario podría experimentar pérdida de información.

Si se rompe el disco duro de tu computadora, si un virus te impide acceder a tu tablet o si te roban el celular, se puede perder la información almacenada en estos dispositivos.

Realizar respaldos en forma periódica asegura que se pueda conservar toda la información almacenada en los dispositivos, como fotografías, videos, presentaciones y documentos de trabajo, entre otros.



Para respaldar tu información, podés utilizar algunos de estos medios:

Disco duro externo

Es buena idea utilizar uno exclusivamente con este propósito para evitar que los datos se borren accidentalmente y pierdas la información.

Dispositivo de almacenamiento USB

Es también recomendable utilizar uno exclusivamente para respaldos y evaluar dónde guardarlo, ya que también debe estar protegido. No es recomendable transportar el dispositivo USB en el mismo bolso de la computadora portátil, ya que en caso de extravío, ambos se perderían.

La nube (internet)

Existen plataformas de almacenamiento en la nube, como Google Drive, OneDrive o iCloud, por ejemplo. Guardando tu información en la nube, podrás acceder a ella a través del celular, computadora o tablet, siempre que tengas conexión a internet.

Configurar y actualizar aplicaciones y antivirus

Para proteger y asegurar la preservación de la información, se debe mantener actualizados y correctamente configurados los equipos y sus aplicaciones.

Un virus puede arruinar tus dispositivos y la información valiosa que contienen. Tener un antivirus instalado y actualizado es tu principal arma para luchar contra malwares y virus. Normalmente, cuando instalás un antivirus, este se configura automáticamente para buscar actualizaciones, pero verificá que se actualice periódicamente.

Casos para analizar y reflexionar

Caso 1: Profesor de Historia

Situación

Durante la hora del recreo, Mauricio, un profesor de Historia, se encuentra en el aula calificando en el portafolio docente. En eso, lo llaman de la Dirección, por lo que debe retirarse unos minutos. Sin embargo, deja la computadora sin bloquear y en ese momento ingresan al aula algunos estudiantes.

Consigna de trabajo

- ¿Qué riesgos implica que el profesor haya dejado la computadora desbloqueada?
- ¿Qué tipo de información está quedando expuesta?
- ¿Qué consecuencias puede tener?

Pautas para la reflexión

- Algunos alumnos pueden cambiar las calificaciones del portafolio.
- Al dejar la pantalla abierta, queda expuesta información confidencial.
- Debemos bloquear los dispositivos cuando no los estamos usando para proteger nuestra información.

Caso 2: Contraseñas seguras

Consigna de trabajo

- Ordená de mayor a menor las contraseñas comenzando por la más segura.
- ¿Cuál es más segura? ¿La contraseña sin sentido o la frase?
- ¿En qué lugar de esa lista ubicarías a tus propias contraseñas? ¿Cuántas contraseñas utilizás?

Pautas para la reflexión

- Una contraseña inadecuada pone en riesgo tu información.
- Utilizar la misma contraseña para tus distintos dispositivos disminuye la seguridad de tu información.
- No utilices contraseñas fáciles de adivinar.
- Una frase puede ser una contraseña segura; cuanto más larga, mejor.

Todas las tardes soleadas voy al parque con mis dos perros

`T l t s v a p c m 2 p`

`A L B E R T O -`

`0 6 0 4 1 9 6 4`

`1 2 3 4 5 6 7 8`

`J c R 2 W 8 0 3`

Para recordar:

- Cuidá tu información sensible y evitá exponerla en ámbitos públicos.
- Evitá usar como contraseña tu nombre personal o de usuario, documento, fecha de nacimiento o cualquier otro dato públicamente conocido.
- Jamás compartas tus contraseñas.
- Recordá bloquear la computadora o la tablet si te alejás momentáneamente.
- Cuando utilices un dispositivo que no es tuyo, evitá seleccionar “Recordar contraseña”.
- Si utilizás una computadora compartida, creá una cuenta diferente para cada usuario.
- Respaldá tu información.
- Instalá un antivirus y mantenelo actualizado.

3

Navegar en internet de forma segura

Temas a abordar:

- Establecer los riesgos de seguridad que pueden presentarse en el uso de internet.
- Brindar herramientas para prevenir riesgos.
- Recomendaciones para navegar en internet de forma segura.

Introducción

Las personas que no están muy familiarizadas con el uso de internet pueden experimentar dudas y temores, por ejemplo, para realizar trámites, compras o búsqueda de información en línea, lo que hace que desistan de utilizar esta herramienta o que la utilicen de manera inadecuada.

Sin embargo, internet ofrece infinitas posibilidades para facilitar muchas de las actividades que se realizan a diario y para obtener la información que se necesita de manera rápida, cómoda y económica. Adoptando medidas básicas de seguridad, se podrá tener una buena experiencia y generar confianza en el uso de la herramienta.

Riesgos de seguridad asociados a navegar por internet

Es importante actuar de manera responsable y consciente en el uso de internet para minimizar los riesgos latentes; de esta manera, se aprovechan aún más las ventajas de la tecnología sin sufrir consecuencias negativas.

¿Cómo identificar páginas web seguras?

Antes de navegar en internet, es imprescindible comprobar que la página es segura, especialmente, si la acción implica brindar datos personales, como por ejemplo, ingresar usuario y contraseñas, usar una tarjeta de crédito o completar formularios con datos de salud.

Existen páginas web que por sus características pueden ser peligrosas, como por ejemplo, las páginas creadas de manera específica por los atacantes o aquellos sitios legítimos que se han infectado.

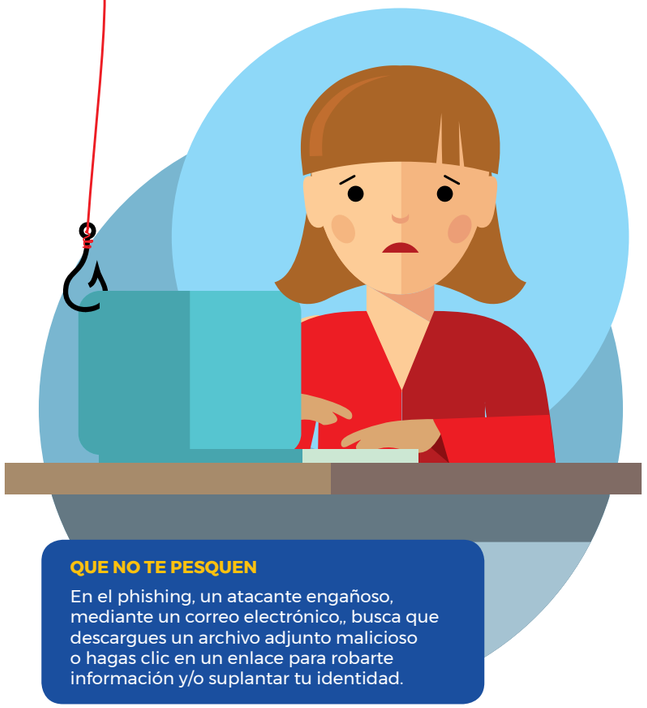
Algunos ejemplos que se pueden encontrar:

- **Sitios para mirar series o películas online.** Estos sitios suelen ser legítimos, pero están habitualmente infectados por virus que afectan los dispositivos desde los cuales se accede. Es importante no acceder a enlaces sospechosos, evitar la ejecución de archivos si no se conoce su seguridad y origen, cerrar las ventanas emergentes (Pop Up) y, si es posible, bloquear su ejecución.
- **Juegos en línea y consolas.** Estos sitios fomentan las comunidades de jugadores, por lo cual se terminan convirtiendo en redes sociales. Se debe tener precaución con quiénes se interactúa en estas plataformas y qué datos se proporcionan.
- **Sitios de compras online y banca electrónica.** Estos sitios suelen ser objeto de suplantación de identidad; en otras palabras, los atacantes crean páginas con una estética similar a la original con el fin de capturar datos de los usuarios *(phishing)*. Por eso es importante verificar no solo que el sitio se vea como habitualmente se lo conoce, sino también que su URL sea la que se espera encontrar.

Phishing

¿Qué buscan obtener los atacantes?

- Datos personales.
- Información financiera.
- Contraseñas.
- Números de tarjetas de crédito.
- Números de cuentas bancarias.
- Que accedas a un sitio web infectado con el objetivo de propagar software malicioso.
- Aumentar el número de visitas que recibe un sitio web a fin de aumentar sus ingresos por publicidad.



QUE NO TE PESQUEN

En el phishing, un atacante engañoso, mediante un correo electrónico,, busca que descargues un archivo adjunto malicioso o hagas clic en un enlace para robarte información y/o suplantar tu identidad.

¿Cómo identificarlos y qué medidas adoptar?

- **Mensajes de contactos desconocidos.** Si no los conocés, mejor no abras sus mensajes, ni lo agregues entre tus contactos.
- **Enlaces a páginas web.** No hagas clic en el enlace si no sabés a qué página te redirigirá.
- **Mensajes en cadena.** No los reenvíes.
- **Publicidades engañosas.** Aparecen a través de carteles (banners o pop ups) que ofrecen ingresar a películas, espectáculos o eventos deportivos en forma gratuita.
- **Robo de identidad.** Una persona se hace pasar por otra persona ante un tercero, normalmente, con una finalidad ilegal o con la intención de causar un perjuicio. Verificá la identidad antes de realizar cualquier acción.
- **Engaños.** Ofertas de trabajo, premios, cupones, sorteos, etc. ¿Recibiste alguna vez un correo que decía que ganaste un viaje o que recibiste una herencia? Es improbable que sea cierto; con seguridad, se trata de un intento de estafa.

Malware

El malware es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. La palabra proviene de la unión de los términos en inglés *malicious software*, que significan “software malintencionado”. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

Existen programas que tienen como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

QUE NO TE AGARREN DESPREVENIDO

El *ransomware* es el equivalente informático a un secuestro. Es un tipo de ataque que te restringe el acceso a la información de tu equipo. De esta manera, el atacante puede exigirte un pago a cambio de quitar esa restricción.

Casos para analizar y reflexionar

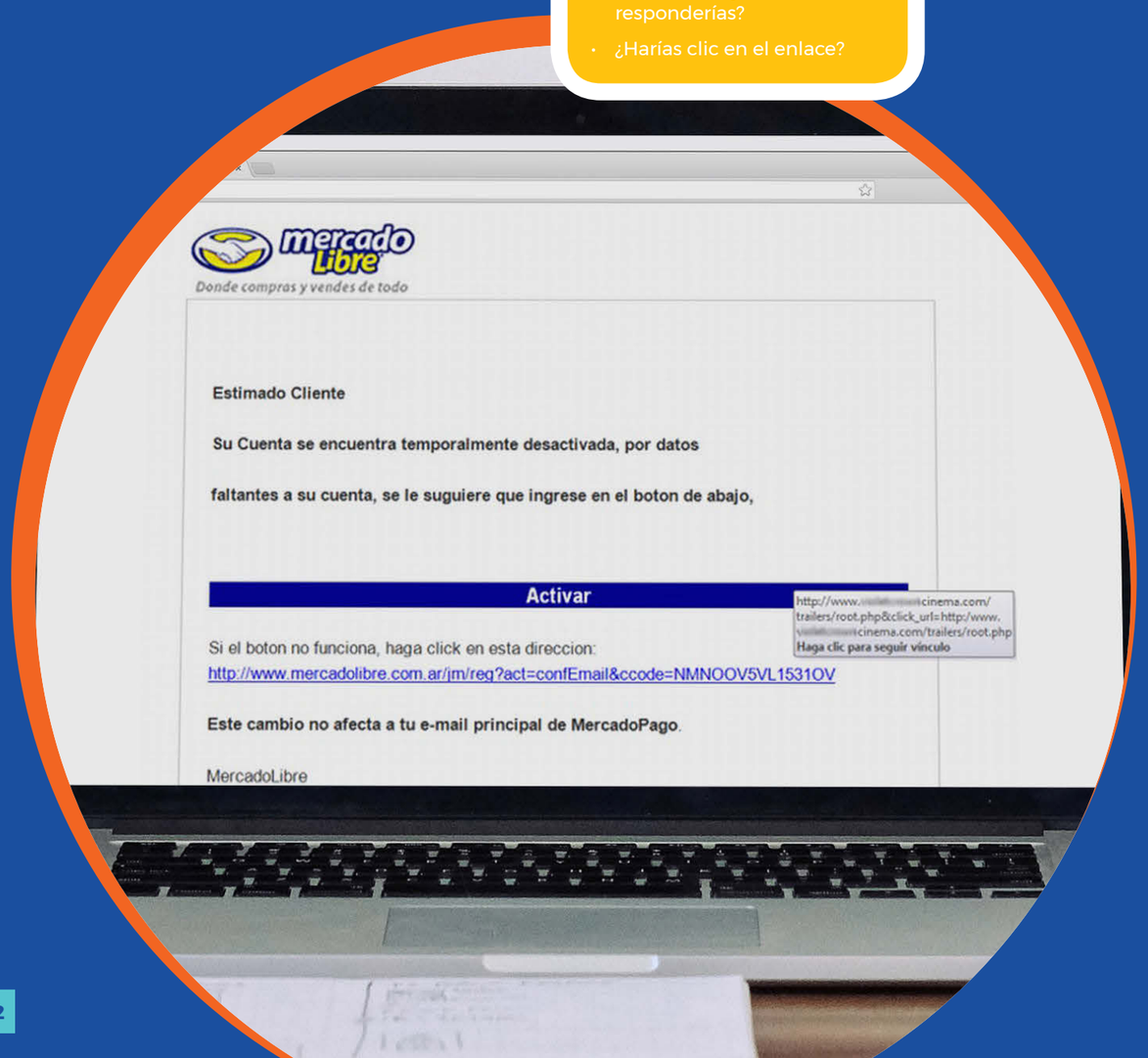
Caso 1: Phishing de correo electrónico

Situación

Te llega este mensaje a tu casilla de correo electrónico, con una URL sospechosa y un texto solicitando actualizar la información de tu cuenta.

Consigna de trabajo

- ¿Hay algún aspecto del correo electrónico que te genere dudas?
- Si te llega este correo electrónico, ¿lo responderías?
- ¿Harías clic en el enlace?



Caso 2: Mensaje de Whatsapp

Situación

El siguiente mensaje circuló a través de Whatsapp; simulaba provenir de una empresa muy conocida y ofrecía trabajo. Luego de enumerar condiciones atractivas, inducen a entrar a un enlace.

Consigna de trabajo

- Si te llega este mensaje, ¿lo responderías?
- ¿Harías clic en el enlace si te atrae alguno de los llamados de esta empresa?
- ¿Hay algún aspecto del aviso que te genere dudas?

Pautas para la reflexión

- La URL del enlace no es segura: **http://**
- No figura el logo de la empresa.
- El enlace no parece ser de la empresa referida.

Conclusión: Se trata de un mensaje falso, que busca que muchas personas brinden sus datos para generar una base de datos con fines desconocidos.

Para recordar:

- Ingresá información personal solamente en páginas web seguras y que conozcas.
- Antes de responder, verificá siempre las direcciones desde las cuales te envían correos electrónicos o mensajes de Whatsapp.
- Leé las políticas de uso y privacidad de los diferentes servicios antes de utilizarlos.
- No abras archivos adjuntos y enlaces de correos electrónicos o mensajes enviados por desconocidos.
- Eliminá correos de remitentes desconocidos.

4

Seguridad en el manejo de dinero (o valores)

Temas a abordar:

- Generar conciencia acerca de la importancia del manejo seguro del dinero y medios de pago electrónicos.
- Brindar información acerca de la protección de cuentas bancarias.
- Identificar las medidas de seguridad para compras en línea.

Introducción

Cada vez existen más soluciones tecnológicas para facilitar la vida cotidiana de las personas. A partir de la Ley de Inclusión Financiera, en Uruguay se promueve el acceso a los servicios financieros de la población y las empresas. Se generaliza, entonces, la utilización de medios de pago electrónicos, como tarjetas de crédito y débito, instrumentos de dinero electrónico y transferencias de fondos. Actualmente, se pueden hacer compras desde el domicilio o cualquier lugar, cobrar el sueldo o la jubilación a través de cajeros automáticos, acceder a cuentas bancarias y realizar trámites y pagos por internet con rapidez y comodidad.

En este capítulo se indican algunas recomendaciones de seguridad básicas para aprovechar estos beneficios y servicios con confianza.

Medidas de seguridad en el manejo del dinero

Uso de contraseñas seguras

Las contraseñas son las claves que permiten tener acceso a tu información financiera. Como estas contraseñas permiten acceder a tu dinero, es importante que tengas el máximo cuidado.

- Estos son algunos de los criterios para configurar las contraseñas de tus cuentas bancarias:
- Utilizá contraseñas complejas: de más de ocho caracteres y que combinen espacios, símbolos, números, mayúsculas y minúsculas.
- Buscá referencias significativas para vos, de modo de poder recordarlas sin problemas.
- Elegí contraseñas que no contengan palabras relacionadas con el sitio utilizado.
- Elegí una contraseña para cada servicio. De esta forma, si se comprometen los datos de una cuenta, no se verán afectadas las demás.
- Cambiá tus contraseñas regularmente y no las compartas con nadie.

Uso seguro de banca electrónica

A través de Internet, podés gestionar pagos, realizar transferencias y controlar los movimientos de dinero de tus cuentas bancarias. Para operar en forma segura, es importante que tengas en cuenta los siguientes aspectos:

- Cerrá la sesión luego de usar tu cuenta.
- Evitá acceder a tu cuenta bancaria desde equipos que no te merezcan total confianza, como computadoras públicas o compartidas.
- Revisá y verificá frecuentemente tus estados de cuenta.
- Evitá utilizar redes wifi públicas para acceder a servicios de banca electrónica.

Uso seguro de las tarjetas de débito y crédito y dinero electrónico

Con el uso de tarjetas de débito y crédito se obtienen muchas ventajas y comodidades:

Tarjeta de débito

Es una tarjeta asociada a una cuenta bancaria.

Trabajadores y pasivos la utilizan para cobrar sueldos, pasividades o prestaciones sociales. También se utiliza para pagar determinados gastos, extrayendo en forma electrónica el dinero de la cuenta bancaria.

Tarjeta de crédito

Es un medio de pago electrónico que permite realizar compras a crédito con financiamiento del banco que otorga la tarjeta.

Dinero electrónico

El dinero electrónico es una forma de representar el dinero en efectivo, por ejemplo, mediante tarjetas prepagas, billeteras electrónicas o instrumentos similares emitidos por instituciones emisoras de dinero electrónico o empresas de intermediación financiera.

CONSEJO práctico

Cuando pagues, nunca pierdas de vista tu tarjeta.

El uso de las tarjetas implica evitar el manejo de dinero en efectivo, lo cual resulta más seguro. Igualmente, su utilización requiere tomar las precauciones necesarias para hacerlo con confianza y seguridad.

A continuación, se enumeran las principales medidas para resguardar tu dinero.

- Evitá perder de vista tu tarjeta de crédito al realizar pagos en locales comerciales.
- No prestes tu tarjeta ni permitas que otras personas la utilicen en tu nombre.
- En caso de robo o extravío de tu tarjeta de débito o crédito, repórtalo de inmediato al banco emisor.
- Al utilizar la tarjeta de débito, evitá que otras personas vean tu PIN al ingresarlo, ya sea cuando vas al cajero automático o cuando comprás en locales comerciales.
- No dejes tus tarjetas expuestas en el auto u otros espacios inseguros.
- Si vas a desechar tu tarjeta, es conveniente destruirla raspando la firma y cortando el plástico en pequeñas partes.

Cuidado del PIN

Es muy importante que protejas tu clave PIN. Si cae en manos de delincuentes, estos pueden acceder a tus cuentas y efectuar retiros o transferencias.

¿Cómo proteger tu clave PIN?:

- No uses 1234, ni números fáciles de adivinar.
- Asegurate de que siempre exista una distancia prudencial entre vos y el próximo usuario.
- Jamás compartas tu PIN.
- No es conveniente que tengas tu PIN escrito en un papel.
- Antes de retirarte del cajero, controlá haber retirado el dinero y la tarjeta.
- Evitá dejar el comprobante de movimiento de dinero en el cajero, ya que tiene el número de tu cuenta, tu saldo y la fecha y hora del movimiento.
- No le pidas a un desconocido que te ayude a operar con el cajero automático. Si tenés dudas sobre cómo hacerlo, solicitá apoyo al banco.

CONSEJO práctico

Al pagar con tarjeta cuidá que nadie vea tu PIN.

¿Te fijaste si el sitio donde comprás en internet es seguro?

ASEGURATE

Si comprás en internet, asegurate siempre de hacerlo en sitios seguros. Para chequearlo, buscá el candado en la barra de direcciones y que diga “https” antes de la dirección web.

Compras por internet

Las compras en línea son un procedimiento que cada vez se utiliza con mayor frecuencia; no obstante, hay que tener claro que al realizar una operación se está brindando información muy sensible, como los datos de la tarjeta o los números de cuenta bancaria.

En las transacciones que se realizan por internet, es fundamental cuidar y mantener determinadas normas de seguridad. Cuidar tu seguridad depende de vos.

¿Qué medidas adoptar para comprar en línea de forma segura?

- Asegurate de comprar siempre en sitios seguros y conocidos.
- Accedé al sitio de la tienda escribiendo la dirección web directamente en el navegador.
- Buscá el candado en la barra de direcciones y confirmá que diga “https://” antes de la dirección web.
- Evitá realizar trámites o compras en línea desde redes wifi públicas. Es más seguro conectarse con los datos móviles del celular.
- No dejes guardados los datos de tu tarjeta de crédito en buscadores y/o plataformas de compra.

Casos para analizar y reflexionar

Caso 1: El abuelo

Situación

Tu abuelo te cuenta que recibió un correo de su banco en el cual se le solicita cambiar la contraseña para poder seguir operando en línea. Confiando en tus conocimientos, te pide ayuda para hacer el procedimiento.

Consigna de trabajo

¿Qué te parece que tenés que hacer? Argumentá por qué.

Pautas para la reflexión

- Los bancos nunca solicitarán modificar datos de cuentas a través de un correo electrónico.
- Verificá siempre la dirección de correo desde la cual te envían la solicitud.
- Ante cualquier duda, lo mejor es contactarse con el banco.

Caso 2: El juego en línea

Situación

Un adolescente llamado Joaquín juega a un juego en línea y para obtener más créditos el sitio le solicita un pago. Entonces Joaquín le pide a su mamá que ingrese los datos de la tarjeta de crédito en el sitio.

Consigna de trabajo

¿Qué debe hacer la mamá de Joaquín y por qué?

Pautas para la reflexión

- No se deben realizar pagos en línea en sitios poco seguros.
- No se debe permitir que ni el navegador ni el sitio almacenen los datos de la tarjeta.

Para recordar:

- Asegurate de comprar siempre en sitios seguros y conocidos.
- Accedé al sitio de la tienda escribiendo la dirección web directamente en el navegador.
- Buscá el candado en la barra de direcciones y confirmá que diga “https://” antes de la dirección web.
- Evitá realizar trámites o compras en línea desde redes wifi públicas; es más seguro conectarse con el 3G/4G del celular o desde la wifi de tu casa.
- No dejes guardados los datos de tu tarjeta de crédito en buscadores y/o plataformas de compra.

5

Redes sociales

Temas a abordar:

- Definir qué es una red social y brindar información acerca de las más usadas.
- Identificar los principales riesgos que presentan.
- Informar cómo configurar mayores niveles de seguridad en cada una.

Introducción

Las redes sociales forman parte de los hábitos cotidianos de adultos, adolescentes y niños como un vehículo para interactuar con otras personas.

El alcance de las redes sociales hace cada vez más necesario estar informados y prevenidos sobre los riesgos que supone interactuar a través de ellas. Como usuarias de las redes sociales, las personas están expuestas a un conjunto de riesgos y amenazas que pueden atentar contra su privacidad e incluso contra su propia integridad.

¿Qué es una red social?

Las redes sociales son plataformas virtuales que permiten la generación de usuarios o perfiles que interactúan dentro de la plataforma y la dotan de contenido.

Las redes sociales se han convertido en pocos años en un fenómeno global; se expanden como sistemas abiertos en constante construcción de sí mismos, al igual que aumentan cada día las personas que las utilizan.

¿Cuáles son las redes sociales más usadas en Uruguay?

Facebook es una red social que conecta personas que comparten la biografía, fotos, actividades, eventos personales. Requiere tener un perfil personal.

WhatsApp es una aplicación de mensajería instantánea a través del celular. Permite enviar mensajes de texto y voz, compartir contenido multimedia y realizar llamadas con conexión a internet.

YouTube permite a los usuarios visualizar, grabar y subir videos sobre distintos contenidos.

Instagram fue creada para que los usuarios compartan fotos y videos. Una de sus principales características es que permite aplicar efectos fotográficos, como filtros y marcos.

Twitter permite a los usuarios enviar y leer mensajes cortos en forma rápida. Es muy usado a nivel empresarial para mejorar el posicionamiento de la marca y es también utilizada por consumidores para hacer reclamos sobre servicios o productos.

Snapchat se usa para compartir mensajes y contenidos que desaparecen en menos de 24 horas.

Otras redes sociales

Existen otras redes sociales que muchos uruguayos han incorporado:

Linkedin es una red que nuclea profesionales con el objetivo de compartir información de interés, generándose redes de contacto e intercambio. Es también utilizada por las empresas como una vía de reclutamiento de profesionales.

Pinterest es una red social muy visual y de atractiva presentación que conecta a las personas en torno a intereses comunes. Lo más visitado son los foros de recetas, comidas, belleza, moda, arte y artesanías.

Spotify es una aplicación a través de la cual se puede reproducir millones de canciones de artistas de todo el mundo.

¿Cuáles son los riesgos en las redes sociales?

Para aprovechar las ventajas de las redes sociales es importante tener en cuenta que el uso inadecuado o irresponsable puede traer problemas de seguridad para vos y otras personas.

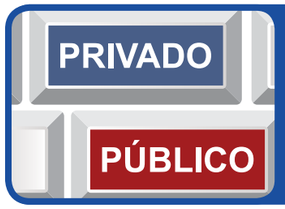
Por eso, es muy importante que conozcas **los riesgos de las redes sociales y cómo prevenirlos.**

¿Conocés los riesgos de las redes sociales?

ASEGURATE

Configurá tu privacidad, no publiques información privada, usá buenas contraseñas y verificá siempre el candado de seguridad en la dirección web.

Amenaza a la privacidad



¿Qué cosas querés mostrar?, ¿con quién vas a interactuar?, ¿quiénes son tus "amigos"?, ¿quién querés que vea lo que publicás?, ¿querés que lo que publicás sea permanente o que se borre con el tiempo?

Generalmente, las personas no se hacen estas preguntas cuando interactúan en las redes sociales, ni toman conciencia de cuánto exponen de su vida privada o de las consecuencias que eso puede tener.

Como usuarios de redes sociales, las personas quieren mostrar a sus contactos momentos especiales, logros, lugares que han visitado y eventos a los que han concurrido, pero antes de hacerlo hay que tener en cuenta que no todos quienes están detrás de una pantalla tienen buenas intenciones.

Configurar la privacidad de tu perfil

- Es muy importante configurar la privacidad antes de subir contenidos.
- Seleccioná con criterio la información de tu perfil.
- Decidí quién puede acceder a tu perfil y a tus datos personales.

Estafas, fraudes, suplantación de identidad

¿Has visto publicados avisos de ofertas espectaculares?, ¿te han invitado a que te inscribas para puestos de trabajo o cursos?, ¿te han resultado sospechosos?

Existe una gran variedad de campañas de fraude difundidas a través de aplicaciones móviles para redes sociales y mensajería instantánea, como Facebook, WhatsApp, Twitter, Instagram y LinkedIn.

Uno de los mecanismos utilizados en este tipo de fraudes es la "ingeniería social", que consiste en crear cuentas falsas o imitar cuentas ya existentes de otras personas o incluso de empresas conocidas. De este modo, los atacantes intentarán engañarte con el fin de obtener datos de inicio de sesión o contraseñas bancarias u obtener dinero.

¿Cuáles son las modalidades más frecuentes?

Estafa de pago anticipado	Los atacantes solicitan dinero por caridad, ofertas de trabajo, oportunidades de negocio o promesas de amor.
Fraude de tarjetas de crédito	A través de la venta de entradas a espectáculos y eventos deportivos, entre otros, los atacantes buscan que realices un pago mediante tarjeta de crédito.
Noticias falsas en Facebook	Los atacantes promueven que hagas comentarios para luego acceder a tus datos.
Publicidad falsa	Los atacantes publican anuncios falsos sobre ofertas y descuentos muy importantes de supuestas empresas conocidas para lograr que respondas.
Dar "me gusta" en páginas de Facebook falsas	Los atacantes ofrecen beneficios en páginas deportivas o de espectáculos, entre otras, para que des información personal.

¿Qué aspectos tener en cuenta para evitar estafas y fraudes?

- Tener precaución frente a mensajes desconocidos.
- Evitá compartir datos o información sensible, como tu teléfono, tu dirección, tu cédula de identidad o tu número de tarjeta de crédito con contactos que no conozcas.
- Desconfiá de los mensajes de supuestos conocidos que te piden dinero.
- Analizá con cuidado antes de responder a las publicidades que aparecen en las redes sociales que ofrecen ofertas impresionantes, regalos, beneficios o cualquier otra ganancia.
- No accedas al pedido de trasladar la conversación a otro canal distinto de Facebook, como por ejemplo WhatsApp, porque estás dando tu número de celular.
- Desconfiá de las personas que afirmen ser amigos o familiares en situaciones de emergencia.
- Antes de compartir información en las redes, pensá bien a quién puede afectar ese contenido, evaluá si tiene información errónea, cuidate y cuidá a los demás.

Acoso y agresiones en línea

Existen varias situaciones que pueden exponer a las personas a situaciones de acoso y agresiones en línea, algunas de las más conocidas son: *cyberbullying, grooming y sexting*.

A continuación te explicamos que es cada una de estas prácticas y como evitarlas.

Cyberbullying

¿Has sido víctima de rumores sobre tu persona que afectan tu imagen?, ¿han publicado una foto tuya que te avergüenza?, ¿qué hacés si recibís una foto o un video comprometedor de alguien?

Estamos ante un caso de *cyberbullying* (o ciberacoso) cuando una persona o un grupo atormenta, amenaza, expone, molesta o humilla a otra persona a través de las redes sociales, correos electrónicos o mensajes de texto. Existe también el ciberacoso que se manifiesta por el excesivo control o violencia entre personas a través de las redes sociales.

Grooming

¿Sabés que existe el acoso sexual hacia niños y adolescentes a través de las redes sociales?

Se llama *grooming* el acoso sexual hacia niños o adolescentes por parte de un adulto en las redes sociales.

Es común que los atacantes generen un perfil falso haciéndose pasar por un niño o adolescente, buscando generar confianza para entablar una relación de amistad.

Luego, suelen pedirle a la víctima fotos o videos con contenido sexual y si no acceden, se producen la presión y el chantaje emocional. El siguiente paso puede ser lograr un encuentro personal.

Estas amenazas exigen que niños, adolescentes y padres estén informados, presten especial atención al tema y sepan cómo protegerse.

¿Sabés con quién estás chateando?

ASEGURATE

Siempre intentá conocer a las personas con las que te comunicás, y si no las conocés bien, no compartas datos personales o información sensible. ¡Cuidate!

Sexting

¿Sabés qué es?, ¿qué impacto tiene?, ¿qué riesgos implica?

El *sexting* consiste en el envío de fotos o videos con contenido sexual de una persona a otra con fines de seducción, por lo general en el marco de una comunicación privada. Esta situación puede generar una gran exposición de la persona y dañar su reputación, pues quien tiene esa información puede hacerla pública en internet.

La red social Snapchat, cuyos contenidos desaparecen en segundos, es un espacio muy utilizado con estos fines. Igualmente, esos contenidos pueden guardarse a través de captura de pantalla o grabarse. El uso de cámaras web durante un chat también puede derivar en una situación de *sexting*.

¿Qué se puede hacer para evitarlo?

- Configurá la privacidad de tu perfil de modo de compartir contenidos solo con tus amigos.
- Evitá compartir datos sensibles, como fotos o videos en los que aparezcas en situaciones comprometedoras.
- Revisá y controlá quién te etiqueta.
- No luches por conseguir “seguidores” o “me gusta” a cualquier costo.
- Comunicate solo con aquellas personas que conozcas, y restringe a ellas el acceso a tu información personal.
- Cuidá tus datos personales o los de tu familia (nombres, dirección, teléfonos); no los compartas por internet.
- No aceptes invitaciones por internet de personas desconocidas o bloquea el acceso a aquellas que no te interesen. Hay personas que mienten acerca de su edad y que podrían engañarte para que les muestres imágenes o videos personales.
- Si empezás a recibir mensajes insultantes o que te molesten en su contenido, cortá toda comunicación con esa persona, e informa de ello a un adulto de tu confianza.
- Si te molestan, guardá los mensajes para poderlos poner a disposición de una autoridad si así lo considera oportuno.
- Igualmente, si ves que es otra persona o compañero el que está sufriendo el ciberacoso no participes de él ni cierres los ojos; avisá a tus padres o profesores para ayudar a frenar el ciberacoso.

- Si te sentís presionado o insultado por alguien no respondas y cortá toda comunicación bloqueándolo en tu lista de contactos.
- No concurras a citas con personas que conociste por intermedio de redes sociales y que no la conocés previamente.
- No utilices cámaras web para chatear con desconocidos, ni envíes fotos tuyas comprometedoras.
- Hablá con personas que puedan estar preparadas, ya sea por su edad o por su profesión sobre el asunto, para que te den indicaciones claras sobre los pasos a seguir para frenar cualquier situación de acoso o agresión.
- También puede ser útil informar a los proveedores de servicios a través de los cuales se haya sufrido el ciberbullying (compañía de Internet, canal de chat, Facebook, Instagram, etcétera) de las actuaciones o mensajes inadecuados para que veten dichos contenidos o al usuario acosador si lo consideran oportuno

Recomendaciones para padres

- Todas las redes sociales tienen una edad mínima para su uso; es importante respetarla.
- Mantenete informado acerca de los riesgos que existen al navegar en internet.
- Entablá un diálogo abierto con niños y adolescentes sobre el tema.
- Transmití la importancia de establecer límites en el uso de las redes sociales.
- Recordá que los juegos en línea también son redes sociales.
- Enseñá a tus hijos u otros niños a configurar la máxima privacidad en las redes sociales.
- Insistí en la importancia de contar con una lista de amigos confiable.
- Analizá en conjunto los riesgos que implica aceptar solicitudes de amistad de personas desconocidas.
- Explicitá los riesgos que implica difundir públicamente datos personales como fotografías, ubicación, número de teléfono y edad, entre otros.
- Prestá atención a las actitudes del niño o adolescente que delaten un cambio de comportamiento.

Casos para analizar y reflexionar

Caso 1: “Demasiada confianza” (sexting)

Situación

María y Santiago tienen 14 años e inician una relación. Comenzaron a mandarse mensajes amorosos hasta que Santiago le pidió a María que le mandara fotografías posando como si fuera una modelo en ropa interior. María no sabía que Santiago le estaba reenviando estas fotografías a Juan, su mejor amigo, quien prometió borrarlas de su celular luego de verlas. Sin embargo, Juan decidió publicar dos de las fotos en una red social. Las fotografías de María se difundieron rápidamente, primero entre los compañeros de clase y luego en otros ámbitos. Los compañeros empezaron a burlarse de María y debido al cambio en su estado de ánimo, sus padres investigaron posibles causas y detectaron el origen de la situación.

Consigna de trabajo

Indicá qué aspectos no tuvo en cuenta María:

- ¿Creés que María pensó que Santiago compartiría sus fotos?
- ¿Creés que imaginó que Juan publicaría sus fotos?
- ¿Qué impacto puede haber causado en María esta situación?

Pautas para la reflexión

- Evitá compartir fotos o videos en los que aparezcas en situaciones comprometedoras.
- Utilizá perfiles privados.
- Definí quién puede ver tu álbum de fotos y tus videos.
- Revisá y controlá quién te etiqueta.

Ficha 1.
Facebook.

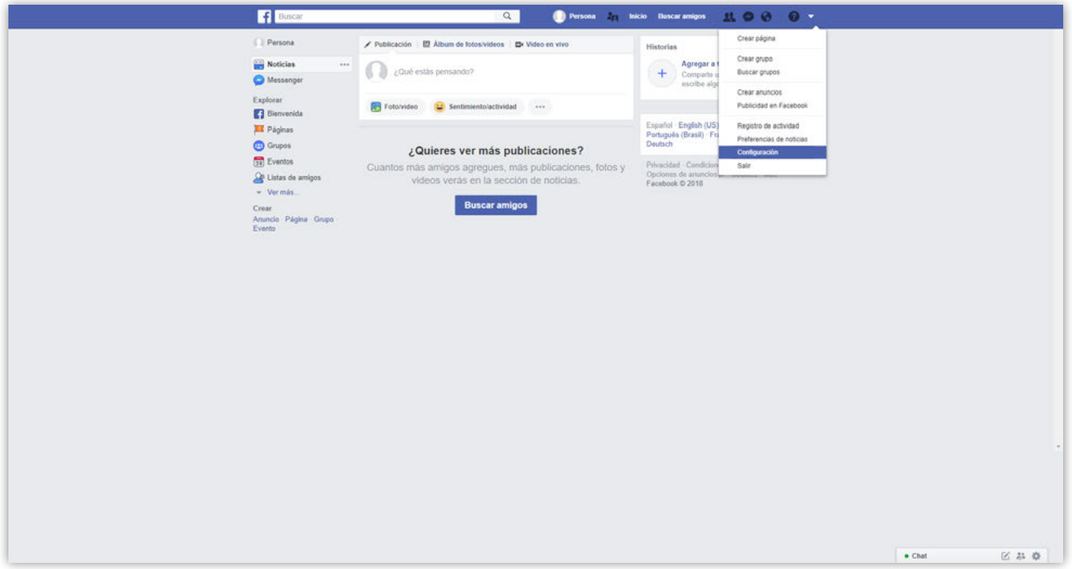
¿Qué es Facebook?

Es una red social mediante la cual podés mantener una comunicación fluida y compartir contenidos (como por ejemplo, fotografías, videos, comentarios e información) de forma sencilla a través de internet.

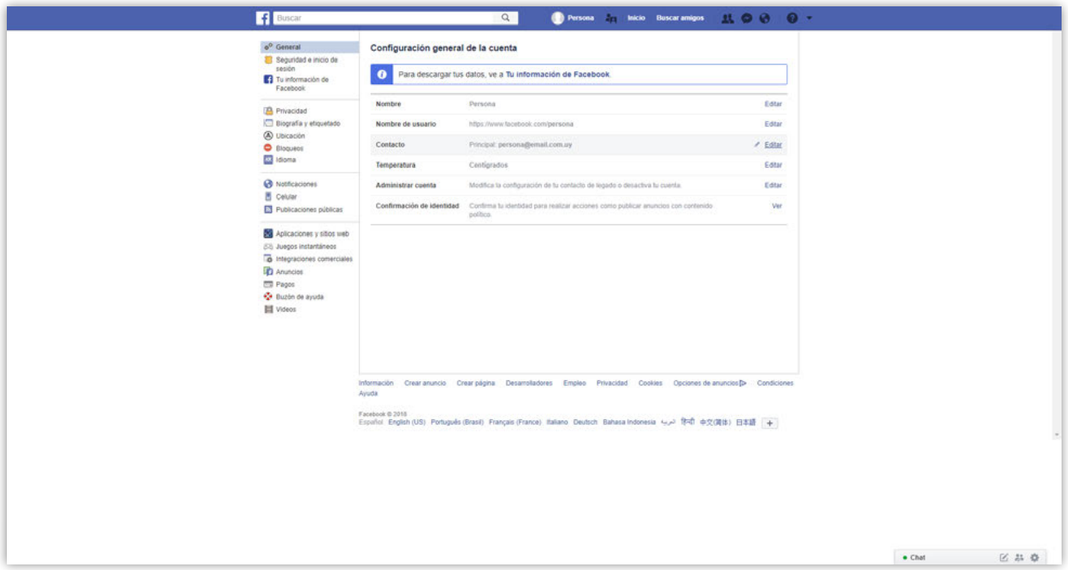
Un uso adecuado de Facebook puede aportarte grandes ventajas para interactuar con otros, pero es recomendable adoptar medidas que te permitan evitar inconvenientes en materia de privacidad y seguridad. En esta ficha se detallan algunas de las principales configuraciones que se deben tener siempre bajo control.

¿Cómo utilizar Facebook de forma segura?

En primer lugar, tenés que ir a la parte superior derecha de la pantalla y hacer clic sobre el ícono con forma de triángulo y luego elegir la opción “Configuración” que aparece en el menú desplegable.



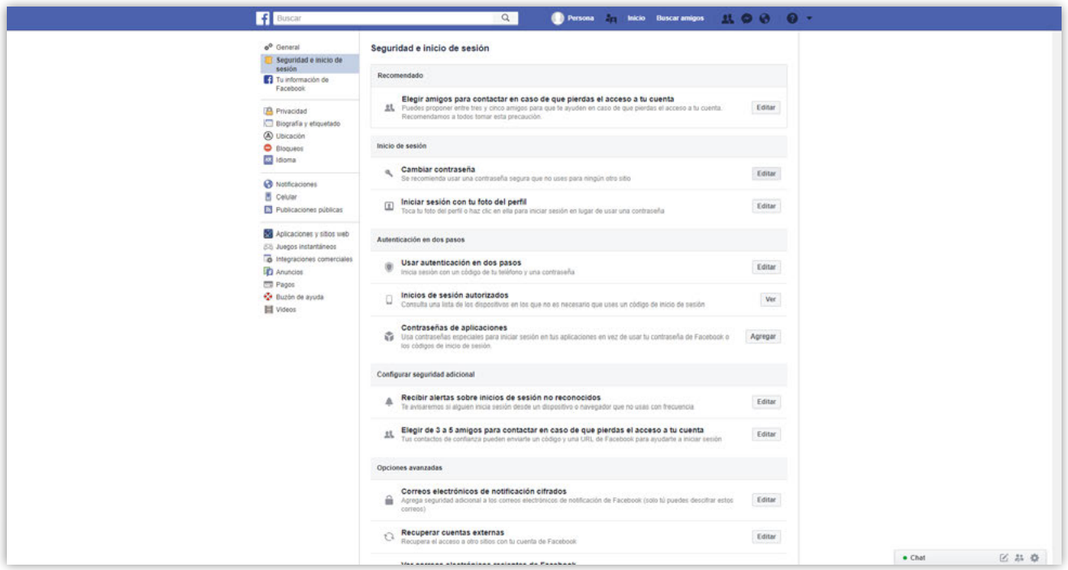
Cuando te das de alta en Facebook, entre los datos que facilitás están tu nombre, correo electrónico y contraseña. Estos datos se pueden cambiar en cualquier momento seleccionando la opción “Editar”.



Es importante que actualices la contraseña con frecuencia, asegurándote en todo momento de que sea segura para evitar que nadie la descifre.

¿Cómo hacerlo?

1. Seleccioná “Configuración”.
2. Hacé clic en “Seguridad e inicio de sesión”.
3. Elegí “Cambiar contraseña” y hacé clic en “Editar”.
4. Escribí una nueva contraseña y seleccioná “Guardar cambios”.

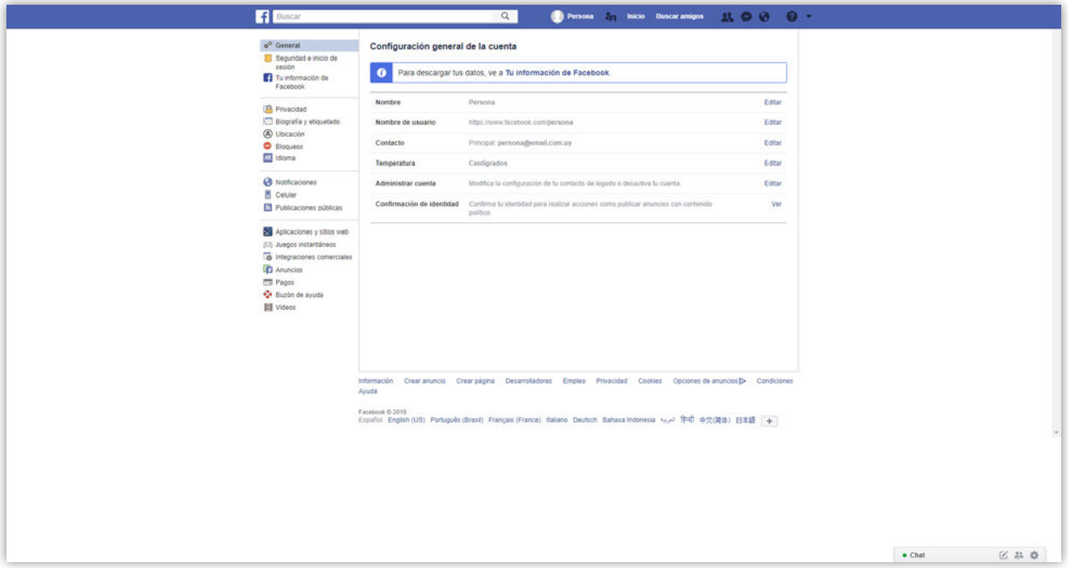


¿Cómo mantener la privacidad en Facebook?

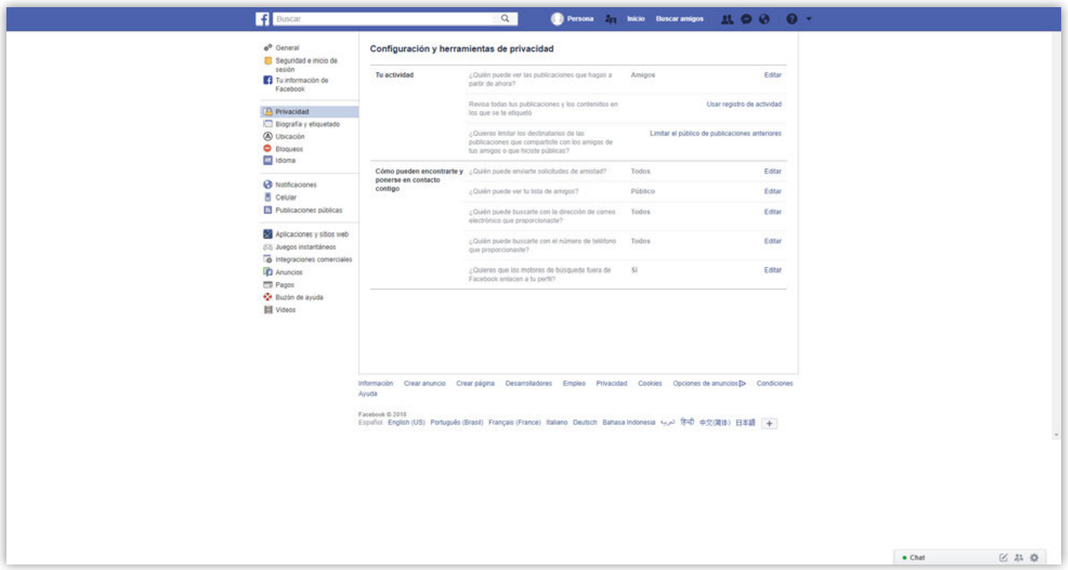
Desde “Configuración”, podés seleccionar “Privacidad” para definir y configurar las opciones que consideres más convenientes.

La configuración recomendable para minimizar los riesgos es la más restrictiva posible.

A continuación, se detallan los aspectos que se pueden configurar para preservar tu privacidad:



¿Cómo elegir quién puede ver las publicaciones?



Para definir si tus publicaciones serán públicas o si solo podrán verlas tus seguidores o un grupo dentro de ellos, tenés que elegir “Privacidad” y seleccionar “Editar”. Allí aparecerá una opción que dice: “¿Quién puede ver las publicaciones que hagas a partir de ahora?”; solo tenés que elegir la opción que prefieras y guardar los cambios.

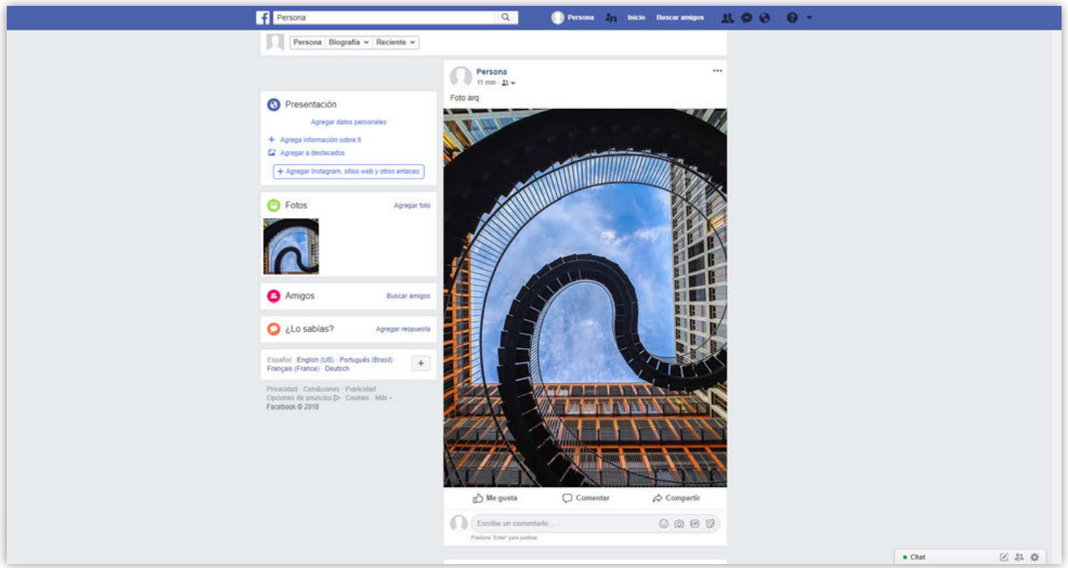
Además, cada vez que vayas a realizar una publicación, podés definir quién puede verlas.

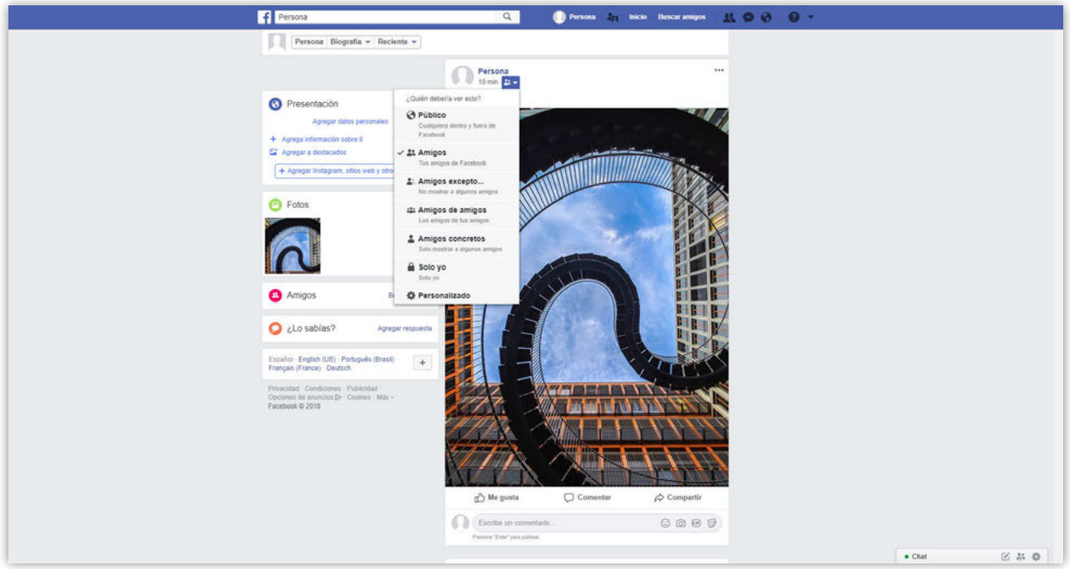
¿Cómo controlar el uso de etiquetas?

Si revisás las fotos y contenidos en los que te etiquetaron y seleccionás “Usar registro de actividad”, aparecen las opciones “Ocultar” o “Eliminar” los contenidos en los que te etiquetaron.

¿Se puede cambiar la configuración de privacidad de publicaciones anteriores?

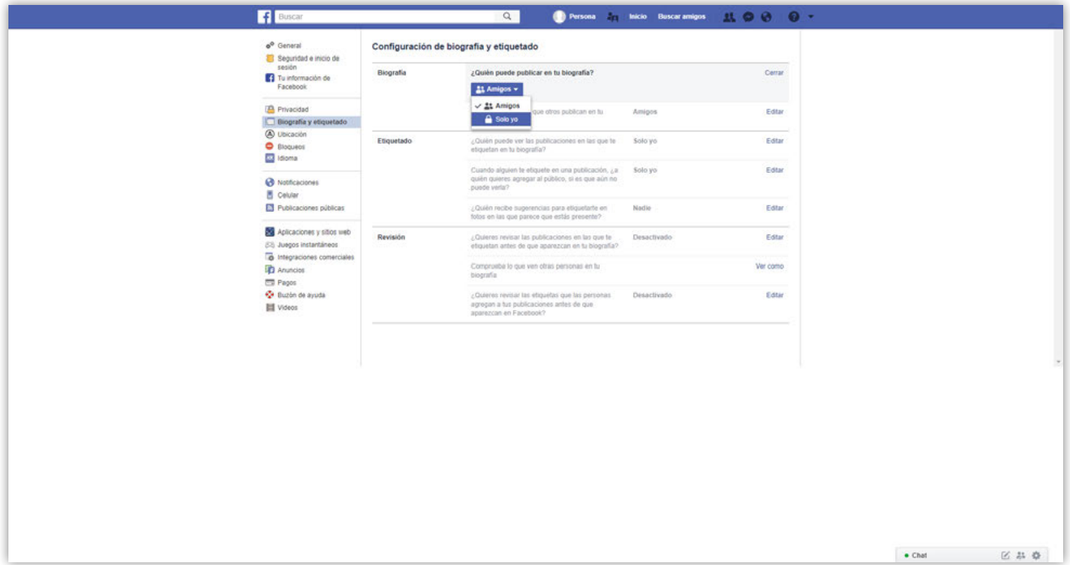
Efectivamente, es posible cambiar la configuración de privacidad de publicaciones anteriores en las que hayas elegido la opción “Público” o “Amigos de amigos” seleccionando “Limitar el público de las publicaciones anteriores” y solo las compartirás con “Amigos”. De todas formas, las personas etiquetadas en esas publicaciones y sus amigos seguirán viéndolas.





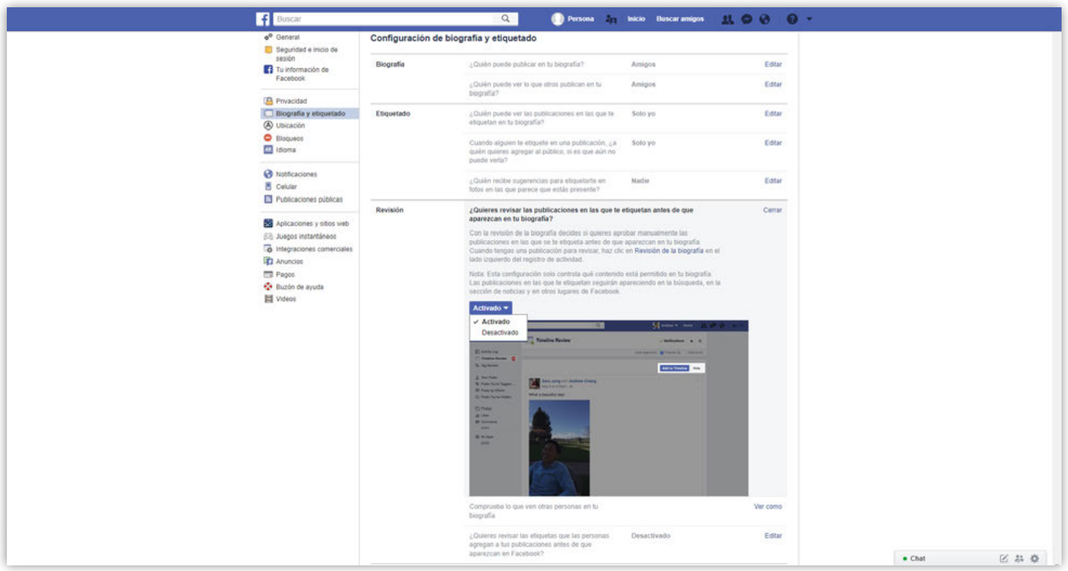
¿Cómo controlar quién puede publicar en la biografía?

Si tenés configurada la opción “Amigos” dentro de “Biografía y etiquetado”, tus contactos y sus amigos podrían publicar en tu biografía. Es conveniente que elijas la opción “Solo yo”; de esa forma, evitás que alguien pueda publicar contenido malicioso en tu perfil.



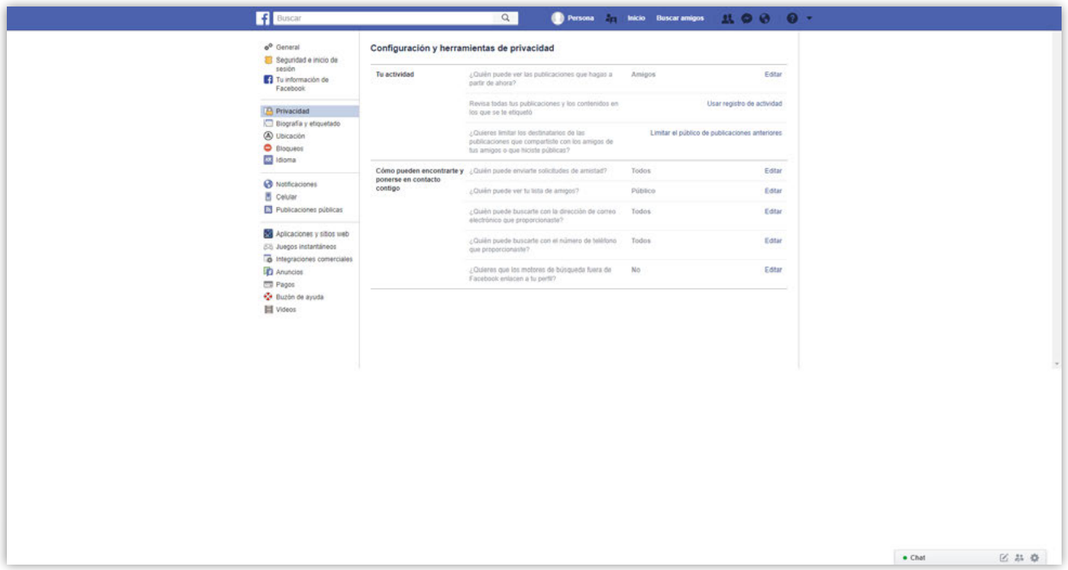
¿Cómo puedo evitar ser etiquetado?

Existe la opción de que revises las publicaciones en las que tus amigos te etiquetan antes de que aparezcan en tu biografía. Para activar esta función, dentro de “Biografía y etiquetado”, se debe ir “Revisión” y elegir la opción “Activado”.



¿Cómo controlar quién puede buscar un perfil?

Si esta configuración está activada, los buscadores pueden enlazar un perfil. Si no querés que cualquiera pueda encontrar tu perfil, es necesario desactivarlo. De esta forma, si alguien te busca a través de un buscador, no te encontrará.



¿Qué se puede bloquear en un perfil?

A través de la opción “Bloqueos”, es posible bloquear todo aquello que no quieras que siga interactuando con tu perfil. Usuarios, mensajes, invitaciones a aplicaciones y eventos y páginas son algunos ejemplos. Para hacerlo, solo tenés que identificar un usuario determinado y hacer clic en “Bloquear”.

¿Qué hacer para bloquear una página?

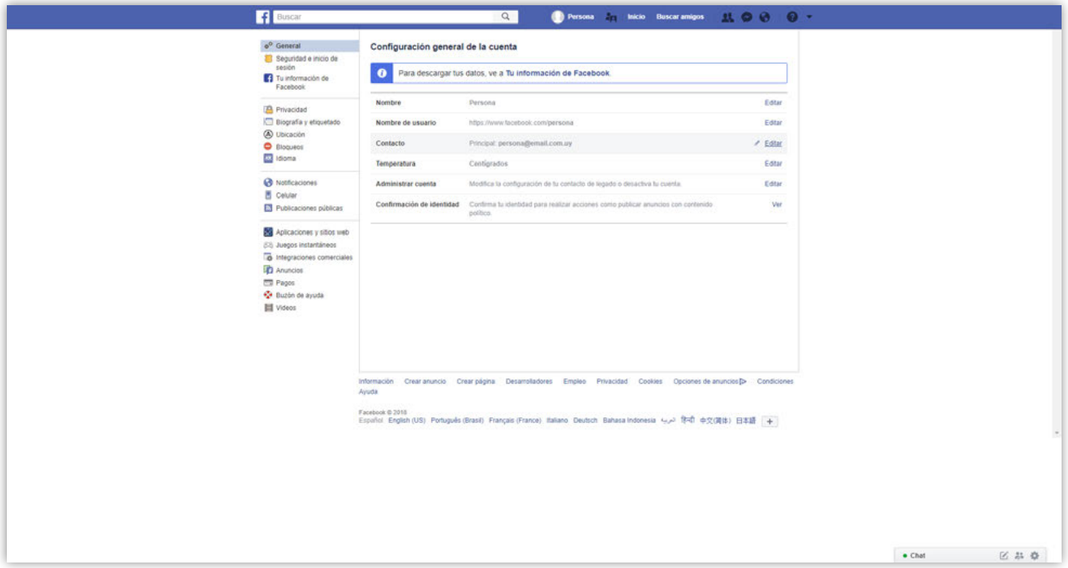
1. Ir a la página que querés bloquear.
2. Hacer clic debajo de la foto de portada de la página.
3. Seleccionar “Bloquear página”.
4. Hacer clic en “Confirmar”.

¿Cómo bloquear a una persona?

1. Hacer clic en la parte superior derecha de la página.
2. Hacer clic en “Accesos directos de privacidad”.
3. Seleccionar “¿Cómo evito que alguien me siga molestando?”.
4. Ingresar el nombre de la persona que vas a bloquear y elegir la opción “Bloquear”.
5. Seleccionar la persona específica que vas a bloquear en la lista que aparece y hacer clic nuevamente en “Bloquear”.

¿Cómo controlar los anuncios que se reciben?

Desde el menú “Anuncios”, Facebook te permite controlar la publicidad y definir si estás dispuesto a recibir anuncios que Facebook te envía en función de tus hábitos de navegación.



Ficha 2.
WhatsApp.

¿Qué es Whatsapp?

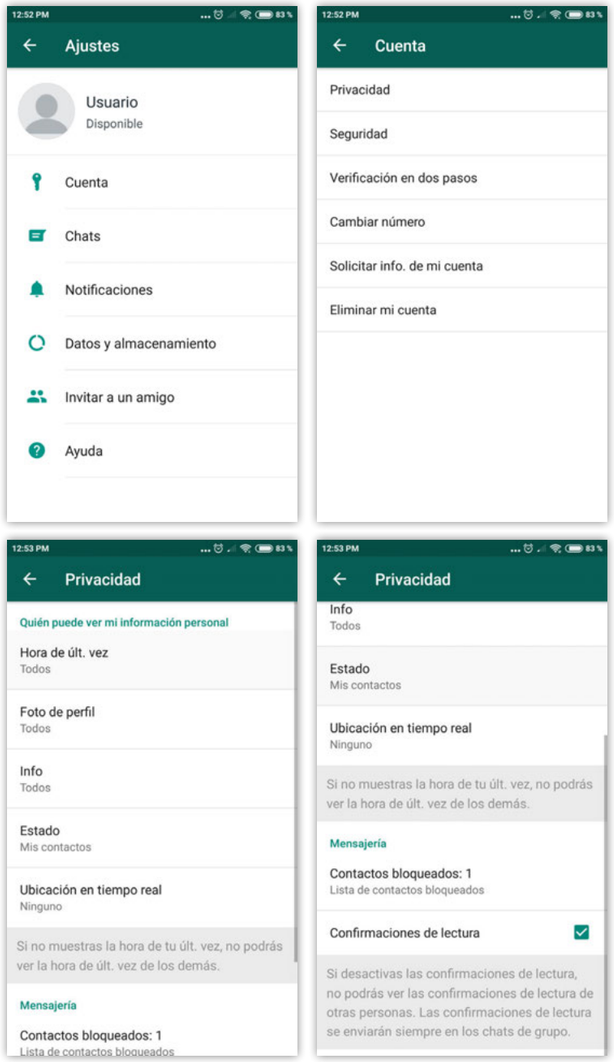
Es una aplicación de mensajería instantánea a través del celular. Permite enviar mensajes de texto y voz, compartir contenidos multimedia y realizar llamadas a través de internet.

Si bien es cierto que Whatsapp es una aplicación segura, tiene algunas medidas de seguridad que no vienen activadas por defecto, por lo que requiere de tu intervención para personalizarlo. Es importante tener en cuenta que cada uno es responsable de mantener la seguridad de su cuenta de Whatsapp.

Configurar las opciones de privacidad

Lo primero que hay que hacer es entrar en la aplicación y pulsar el ícono “Ajustes” en los dispositivos Android y “Configuración” en los dispositivos IOS (iPhones y iPads).

Luego, hay que ingresar a la opción “Cuenta” y seleccionar “Privacidad”, donde se encontrarán los ajustes para configurar la visualización de la hora de última conexión, foto de perfil, estado y la posibilidad de bloquear contactos.

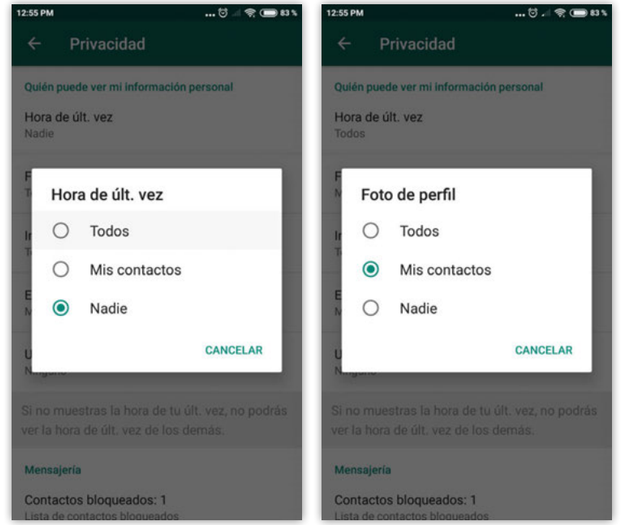


¿Se puede elegir con quién compartir información?

Es posible elegir si querés compartir la hora en que te conectás y con quién seleccionando “Última vez” y luego, escogiendo una de las siguientes opciones: “Todos”, “Mis contactos” o “Nadie”.

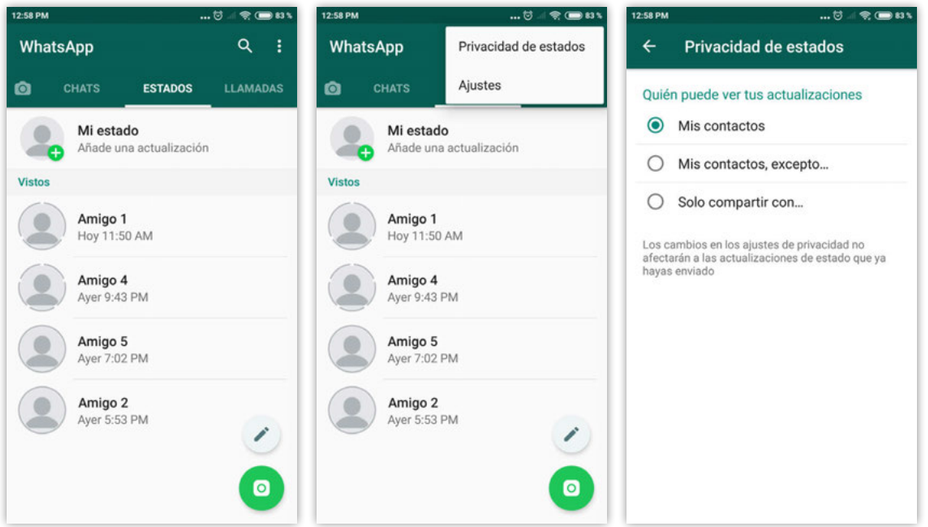
Si seleccionás “Nadie”, no podrás ver la hora de la última conexión del resto de usuarios.

También podés configurar quién puede ver tu foto y tu información de perfil seleccionando las opciones: “Foto de perfil” e “Info”. También podés configurar quién querés que tenga acceso: “Todos”, “Mis contactos” o “Nadie”.



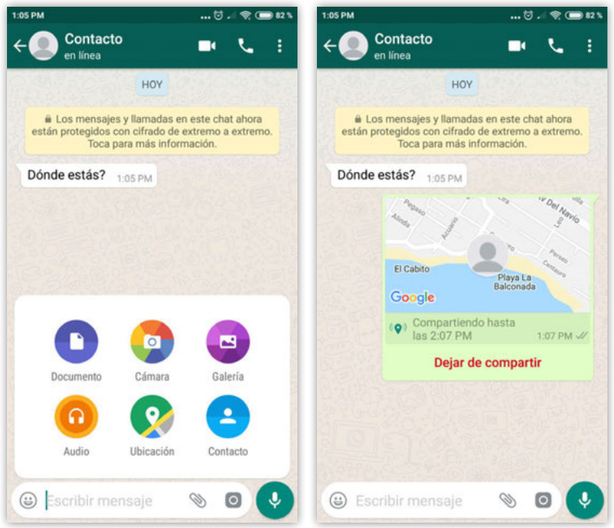
Los “estados” permiten compartir textos, fotos y videos que desaparecen a las 24 horas de ser publicados.

Whatsapp tiene configurado por defecto que recibas actualizaciones de estado de tus contactos y que cualquier usuario que tenga tu número de teléfono reciba las tuyas. Si no querés que cualquier persona pueda ver tu estado, es importante que configures alguna de estas opciones:



¿Cómo definir si se quiere compartir la ubicación?

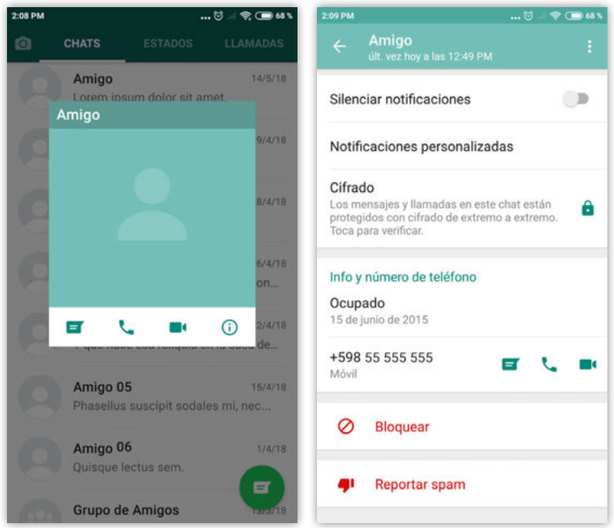
Se puede elegir la opción de compartir o no la ubicación donde te encontrás. La función "ubicación en tiempo real" permite compartir tu ubicación precisa con tus contactos o grupos durante un período de tiempo específico. Seleccionando el ícono del clip, se despliega el siguiente menú:



Es importante configurar adecuadamente la privacidad; de lo contrario, compartir tu ubicación puede representar importantes riesgos para vos y quiénes estén contigo, ya que se brinda mucha información, especialmente, cuando estás de vacaciones o fuera de tu casa.

¿Cómo bloquear usuarios?

En cada conversación con un contacto, puedes ir al menú y encontrarás la opción "Más" y luego "Bloquear" que, como su nombre lo indica, permite bloquear a aquellos usuarios que prefieres que no se contacten contigo a través de la aplicación. Los contactos bloqueados no podrán llamarte o enviarte mensajes.



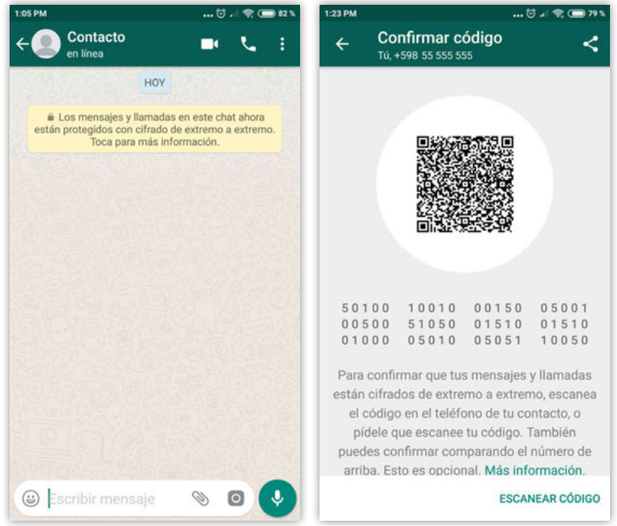
Confirmación de lectura

Esta función te permite saber si tus contactos leyeron los mensajes que les enviaste y ellos podrán saber si vos leíste los que te enviaron. Si lo desactivás, nadie accederá a esta información.

Configurar las opciones de seguridad

La última versión de esta red social trae configuradas medidas de seguridad que se denominan "cifrado extremo a extremo", que permiten mayor confidencialidad en las conversaciones en Whatsapp. Para comprobar que la conversación está cifrada, tenés que hacer clic sobre el nombre del contacto con el que quieras chatear y aparecerá un mensaje que indicará si la conversación está cifrada o no.

El cifrado asegura que solo vos y la persona con la que te estás comunicando puedan leer la conversación; ni siquiera Whatsapp puede hacerlo. Tus mensajes estarán asegurados con un candado y solo vos y el receptor tienen el código/llave para abrirlo y leer los mensajes.



Ficha 3.
Instagram.

¿Qué es Instagram?

Es una aplicación y una red social para subir fotos y videos. Una de sus principales características es que ofrece la posibilidad de aplicar efectos fotográficos, como filtros y marcos. Con Instagram podés tomar fotografías y modificarlas con efectos especiales para luego compartirlas también en otras redes sociales.

Instagram también cuenta con una función conocida como “Instagram Stories”, que ofrece a los usuarios la posibilidad de crear publicaciones que desaparecen luego de 24 horas desde su publicación, al igual que ocurre en la aplicación Snapchat.

¿Cuáles son los riesgos?

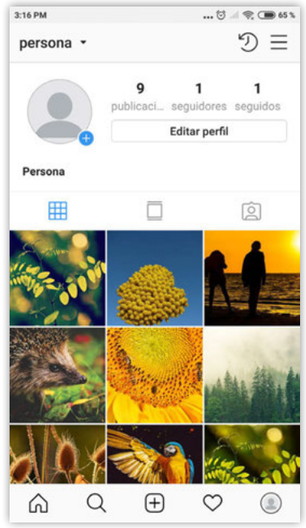
Su mayor riesgo es darle mucha exposición a tu vida cotidiana. Para evitar hacer pública más información de la conveniente, es recomendable configurar de forma correcta las opciones de privacidad y seguridad de la aplicación.

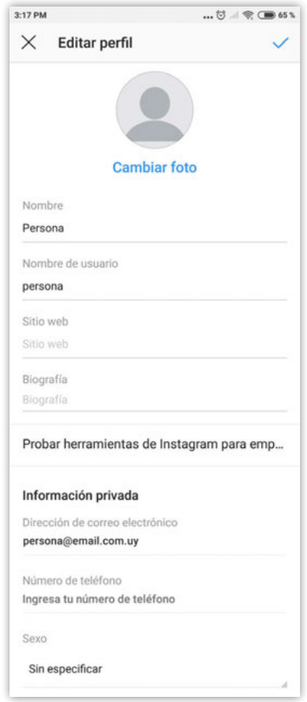
¿Qué medidas de seguridad se pueden adoptar?

La configuración por defecto de Instagram permite que cualquier usuario pueda ver las fotos y videos que publiques sin ningún tipo de restricción. Esta configuración es riesgosa, ya que un usuario malintencionado puede obtener información valiosa que podría usar en tu contra. Para prevenir estas situaciones, se debe configurar la privacidad:

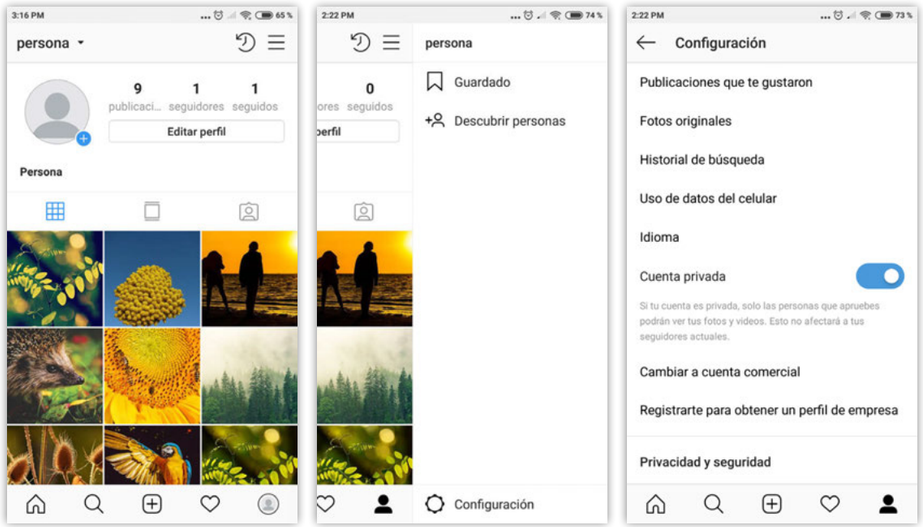
Editar perfil

Es importante que tengas en cuenta que el único dato obligatorio requerido es el nombre de usuario. En caso de que hayas introducido otros detalles que quieras eliminar (como por ejemplo, tu número de teléfono, tu dirección o tu biografía), es posible borrarlos fácilmente desde la pestaña “Editar perfil”.





Para evitar que tu perfil sea público y cualquier persona pueda acceder a contenidos que publiques, es necesario activar la opción “Cuenta privada”. Esta opción te permite configurar que únicamente los seguidores que hayas aprobado puedan ver tus contenidos.

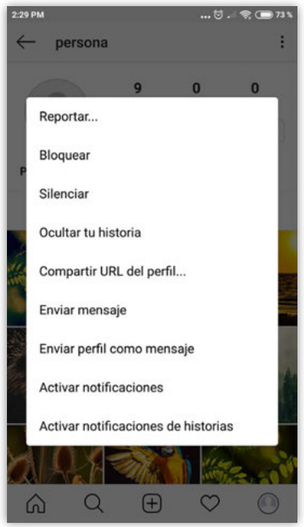


Bloquear usuarios

Instagram permite que en apenas unas horas puedas incrementar tus seguidores en varios miles y esto puede darte la sensación de que tenés un perfil muy popular. Sin embargo, como en todos los casos, perder el control sobre tu privacidad tiene sus riesgos.

Hay personas que se dedican a generar *spam* en Instagram, dando demasiados “me gusta” y haciendo comentarios en tus fotografías. Estos usuarios te siguen y dejan de seguirte constantemente.

Para bloquear usuarios, lo primero que tenés que hacer es ir al perfil de esa persona y seleccionar la opción “bloquear”. Si estás viendo una de las fotos que ha publicado, con pulsar su nombre irás al perfil de usuario y podrás bloquearlo.



¿Qué hacer frente a conductas abusivas de algún usuario?

También puede darse el caso de que un seguidor que hayas aprobado tenga conductas abusivas contra tu persona, para lo cual también tenés la opción “Bloquear usuario”.

Además, Instagram te permite denunciarlo. Para denunciar a un usuario, tenés que seleccionar a la persona que querés denunciar, seleccionar “Reportar...” e indicar los motivos por lo que realizaste la denuncia.

¿Cómo configurar la privacidad de ubicación?

Instagram tiene configurada la localización de forma automática; cualquiera puede averiguar mucha información sobre los lugares que frecuentaste y tus hábitos y podría hacer un mal uso de estos datos.

Para evitar que todos sepan tu ubicación, tenés que eliminar la “localización” antes de seleccionar “publicar”.

Lo más recomendable es utilizar la geolocalización según tu necesidad o interés y ser consciente de lo que supone activarla o desactivarla. Es importante que tengas en cuenta:

- El mapa de fotos permite ver la posición geográfica de tus fotos.
- Esa información podría ser usada para recopilar datos acerca de vos.
- Los datos de localización geográfica revelan tus hábitos y patrones de conducta
- Esta información puede ser usada para perjudicarte.

Ficha 4.
Snapchat.

¿Qué es Snapchat?

Es una aplicación de mensajería instantánea muy utilizada por adolescentes destinada al envío de mensajes multimedia. Su principal característica es la mensajería efímera, donde las imágenes y mensajes pueden ser accesibles solo durante un tiempo determinado elegido por los usuarios.

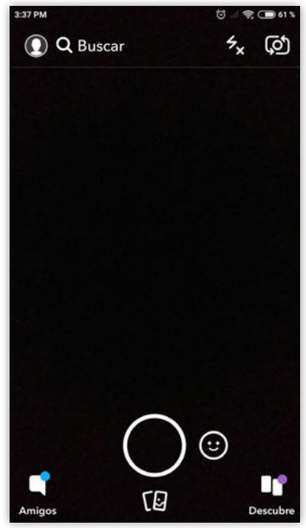
¿Es posible borrar definitivamente la información?

Cualquiera de los amigos con los que compartís mensajes en Snapchat puede hacer una captura de pantalla (en tal caso, se recibe una notificación) o grabar el video en otro dispositivo y compartir esa información con terceras personas. De manera que es falso pensar que la información transmitida por Snapchat no se conserva en ningún caso.

¿Cómo configurar privacidad en Snapchat?

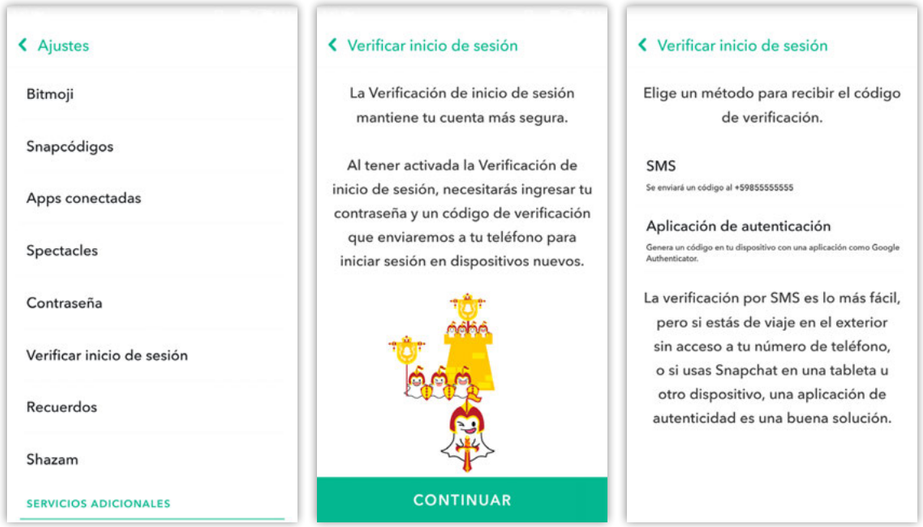
Desde el ícono del fantasma que aparece en la parte superior de la interfase, podés acceder a las opciones de privacidad de la aplicación.

En el nuevo menú que aparece se encuentran las opciones de privacidad.

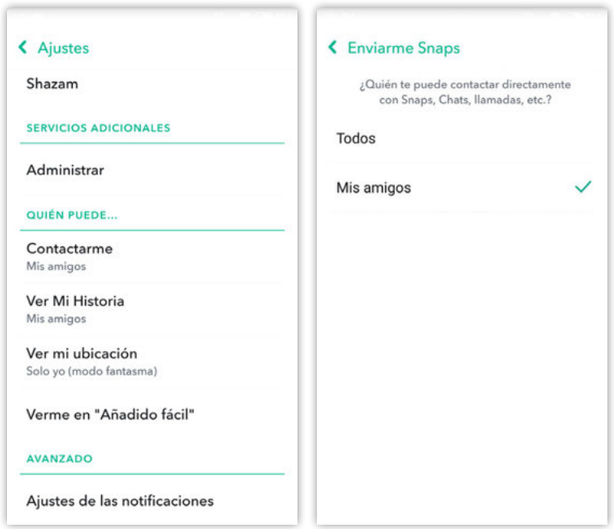


¿Por qué usar el código de verificación?

Como en el resto de las redes sociales, es importante que cada vez que inicies sesión en un nuevo dispositivo, además de introducir el nombre de usuario y la contraseña, ingreses un código de verificación que recibirás a través de un SMS. La verificación de inicio de sesión es muy importante para proteger tu cuenta en caso de que alguien consiga tus claves de acceso.



¿Quién puede contactar?



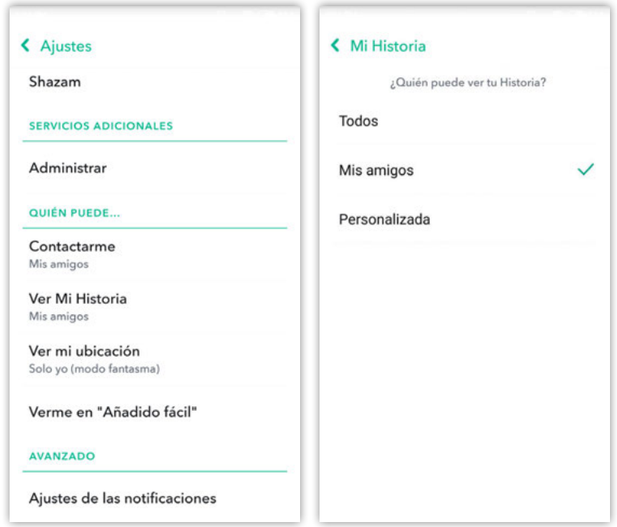
Para configurar qué usuarios de la aplicación pueden establecer contacto contigo, utilizá la opción “Quién puede contactarme”, para luego seleccionar “Todos” o solo “Mis amigos”. Asegurate de que conocés a todas las personas que figuran en tu lista de amigos y que la persona con quien te comunicás es quien dice ser. Si alguien intenta agregarte, es importante que tengas certeza de que conocés a esa persona antes de aceptar su solicitud de amistad.

A tener en cuenta:

- Incluso al seleccionar “Mis amigos”, cualquiera con quien estés en un grupo se podrá comunicar contigo. Para ver quién está en un chat grupal, pulsá el nombre del grupo en la pantalla del chat.
- Si te invitan a participar en una “Historia Grupal”, se te indicará si hay alguien en dicha historia a quien bloqueaste. Si optás por participar, esa persona podrá ver tus snaps.
- Si seleccionas “Todos” en “Quién puede contactarme”, incluso los snapchatters que no añadiste podrán enviarte snaps y chats.
- Si querés recibir snaps de “Todos” pero notificaciones solo cuando tus “amigos” te envían snaps, podés cambiar tus ajustes de notificaciones en Ajustes > Notificaciones.

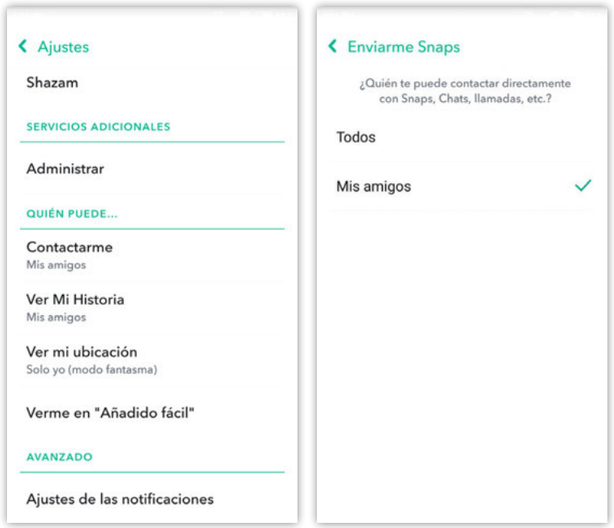
¿Cómo proteger contenidos y seguridad en Snapchat?

Para ello, es necesario que te asegures de estar compartiendo las cosas que publicás en “Mi historia” solamente con tus amigos. Además, asegurate de que conocés a todas las personas que figuran en tu lista de amigos. Para configurar quién accede a tus contenidos, seleccioná en “Ver mi historia” alguna de las siguientes opciones: “Todos”, “Mis amigos” o una lista personalizada. Es recomendable que facilites esta información únicamente a tus contactos conocidos.



¿Qué datos puedo reservarme?

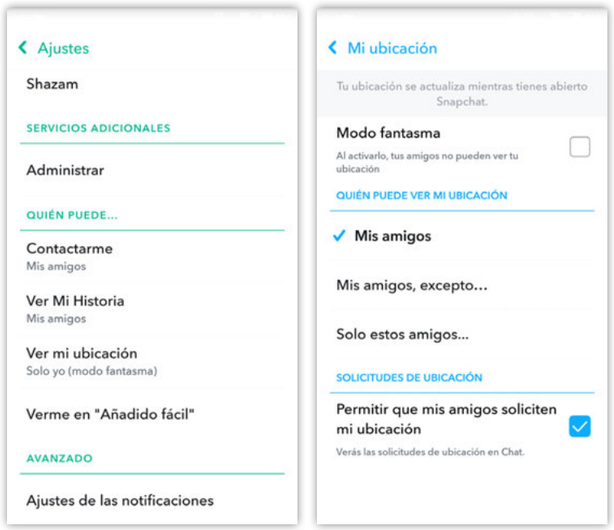
Por ejemplo, la opción cumpleaños te permite mostrar a tus contactos la fecha de cumpleaños, pero no el año, de esa forma no revelás tu edad.



¿Cómo configurar la geolocalización de forma segura?

Es posible configurar la opción de que identifiquen tu ubicación en el momento. Es recomendable que evalúes quiénes estarían viendo tu ubicación en ese momento y su conveniencia. Cuanto más personalices la información que compartís, menores serán los riesgos a los que te expondrás.

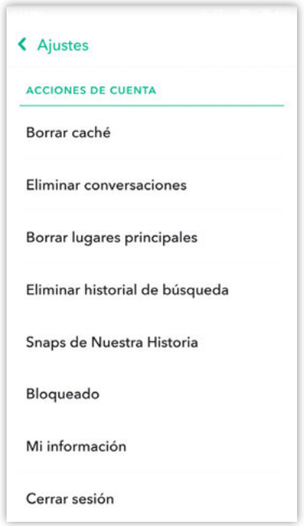
Podrás elegir entre tres opciones: “Solo yo” (modo fantasma), “Mis amigos” y “Seleccionar amigos”. Una vez que hayas indicado la privacidad de Snap Map, podrás finalizar la configuración. En este momento, tendrás acceso al mapa interactivo, en el que podrás verte a vos mismo y a todos tus amigos que también hayan decidido compartir su localización contigo.



Además, Snapchat ofrece otras funcionalidades que contribuyen a la seguridad:

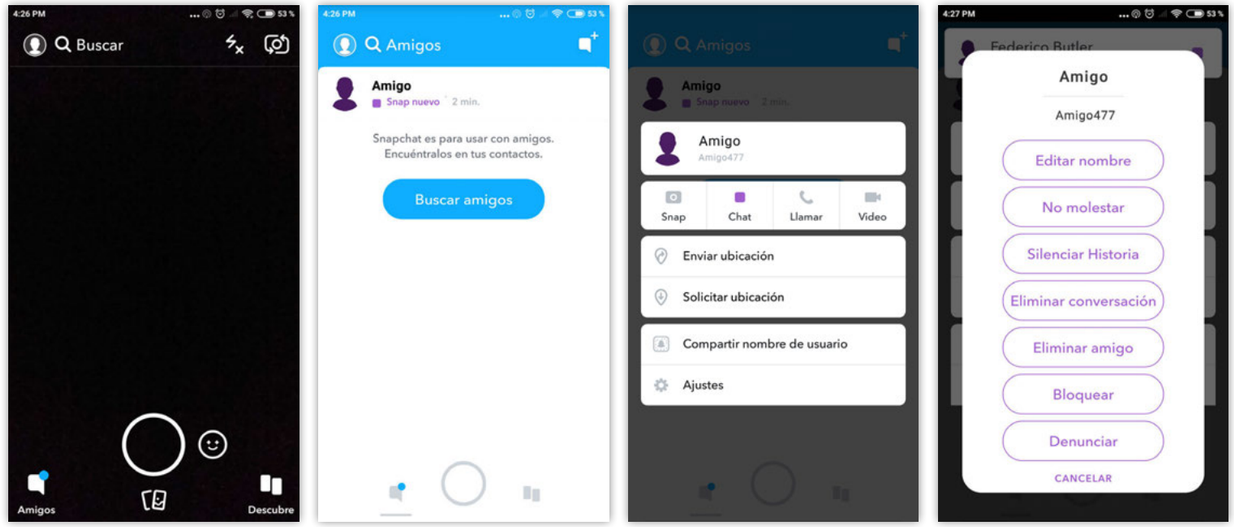
1. Eliminar conversaciones

Es conveniente eliminar con frecuencia el historial de conversaciones, como muestra la imagen:



2. Bloquear usuarios que te estén molestando.

Buscá al usuario que deseás bloquear, seleccionalo y pulsá sobre el ícono con forma de engranaje para que aparezca la opción “Bloquear” o “Eliminar”.



Ficha 5.
Twitter.

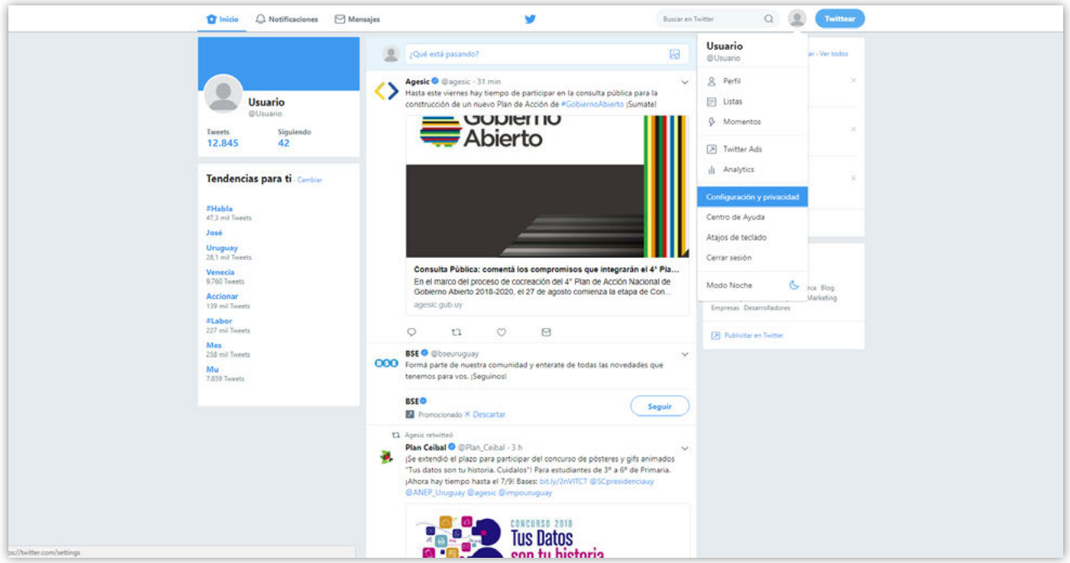
¿Qué es Twitter?

Es una red social cuya principal característica es permitir publicar mensajes limitados a 280 caracteres. Estos mensajes son conocidos como *tuits*. A diferencia de otras redes sociales, Twitter tiene como particularidad que mucha de la información de sus usuarios es pública. De todas formas, permite añadir opciones de privacidad.

¿Cómo configurar quiénes pueden leer un tuit?

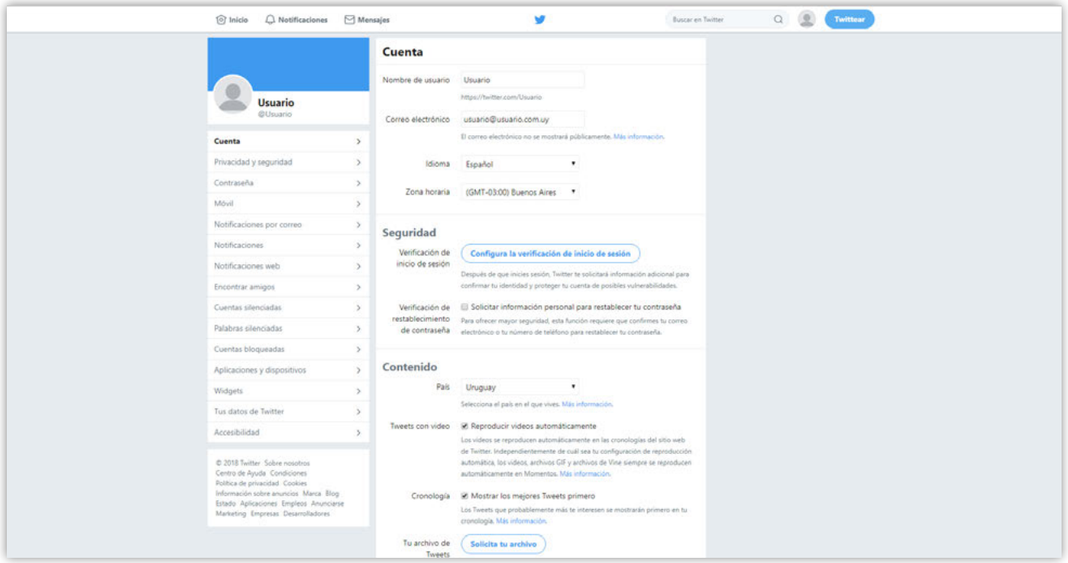
Twitter configura los tuits de forma predeterminada como públicos, por lo que cualquier persona, tenga o no cuenta en Twitter, podrá verlos. Si no querés que esto sea así, podés configurar tus tuits para que solo los lean aquellos usuarios que hayas aceptado para seguirte.

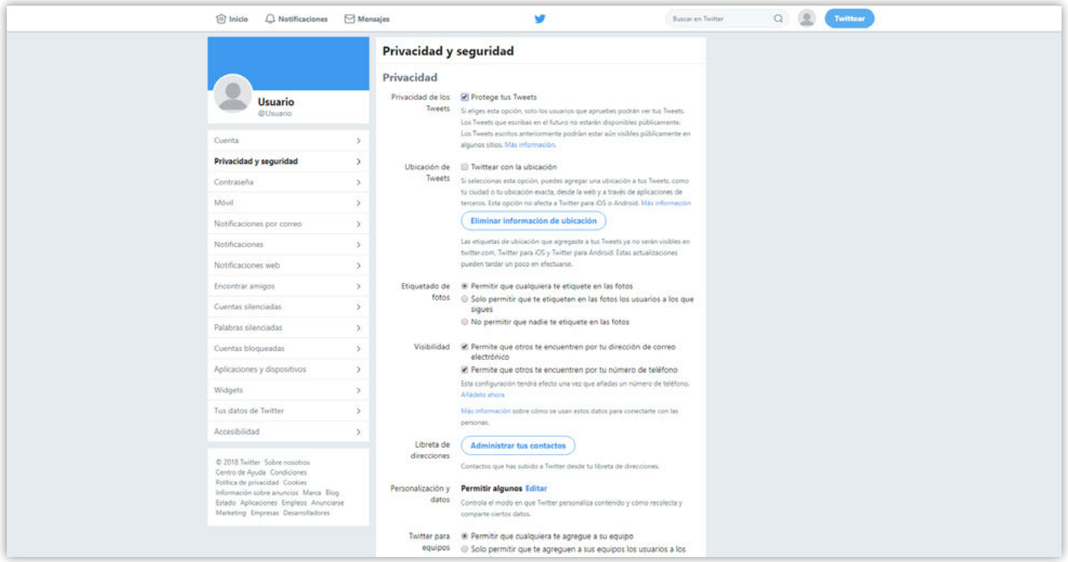
En la parte superior derecha de la pantalla, tenés que hacer clic en tu imagen de perfil y, a continuación, en “Configuración”. En el nuevo menú que aparecerá, seleccioná la opción “Configuración y privacidad”.



¿Qué información se quiere mostrar?

Para revisar la información que estás mostrando, tenés que ir a tu imagen de perfil pequeña arriba a la derecha, hacer clic en “Privacidad y seguridad” y marcá la casilla “Proteger mis Tweets”.

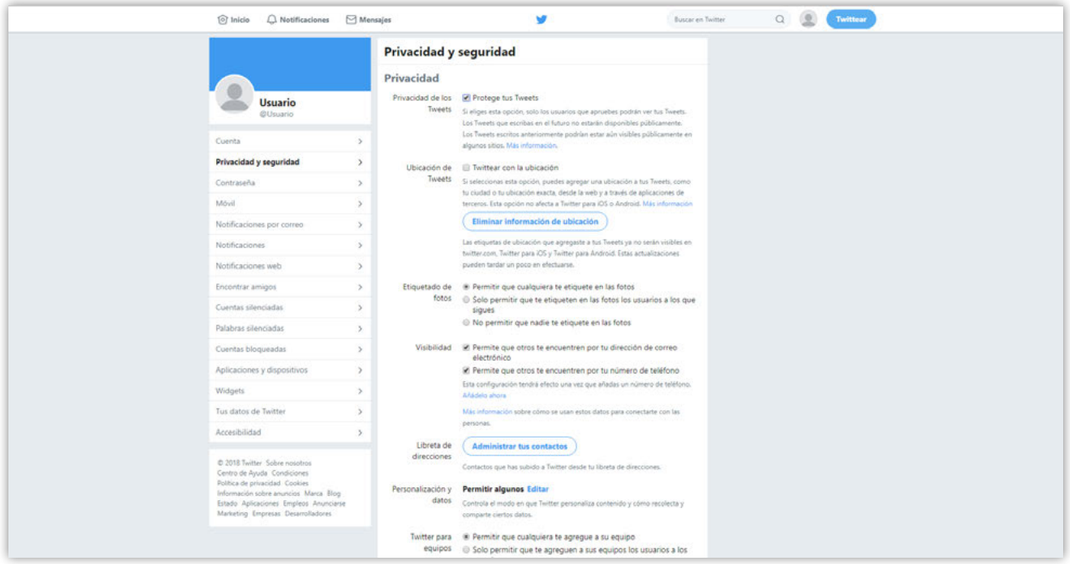




¿Es seguro configurar la geolocalización?

La geolocalización es muy útil para obtener la ubicación exacta de lugares y objetos (por ejemplo, cuando se pierde el celular), lo cual la vuelve una valiosa herramienta.

Sin embargo, hacer públicos nuestra ubicación y movimientos puede aparejar ciertos riesgos, ya que no se sabe quién puede estar manejando esa información y con qué fines. De hecho, es una característica que está deshabilitada por defecto en Twitter. Si en algún momento la has tenido activada, podés desactivarla e incluso borrar todo el historial de geolocalización desde la función “Borrar toda la información de ubicación”.

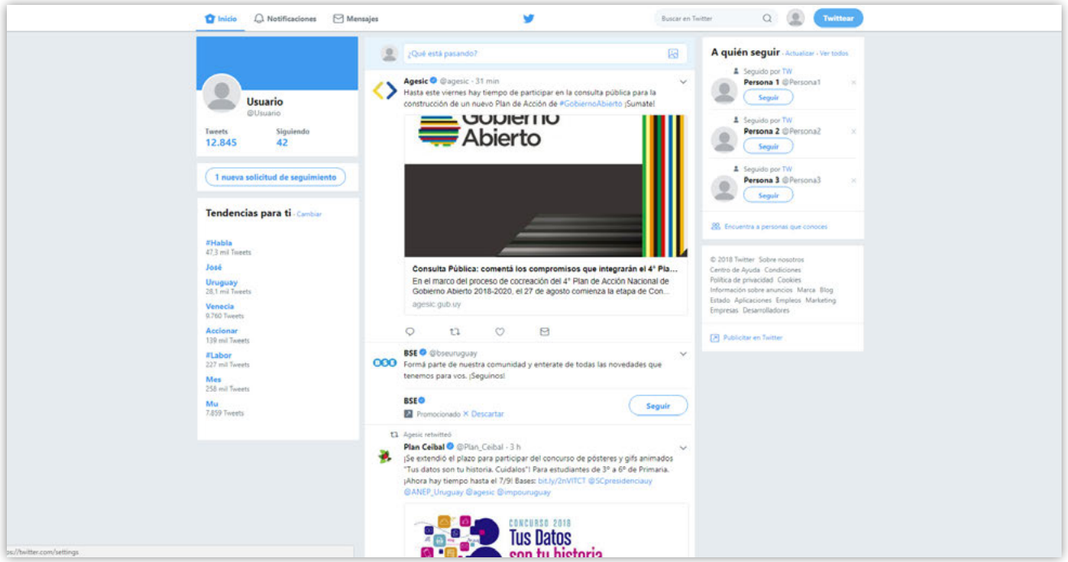


¿Se puede deshabilitar la recepción de anuncios?

No es posible deshabilitar la recepción de anuncios en Twitter. Si no querés ver un tuit promocionado, podés simplemente eliminarlo de tu cronología. Para ello, tenés que seleccionar “No me gusta este anuncio”, pero no podrás deshabilitar la opción de ver anuncios en la cronología.

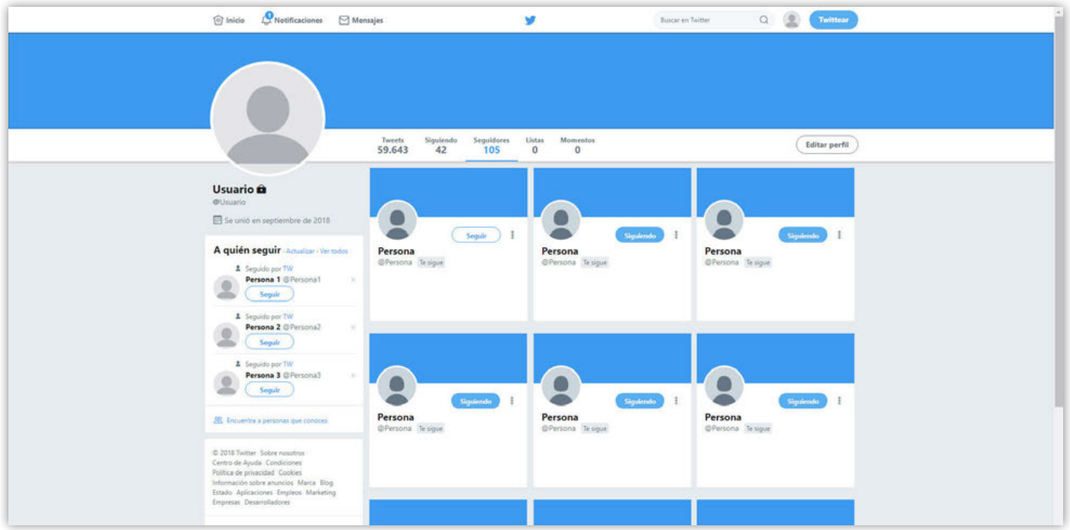
¿Cómo aceptar o rechazar nuevas solicitudes de seguidores?

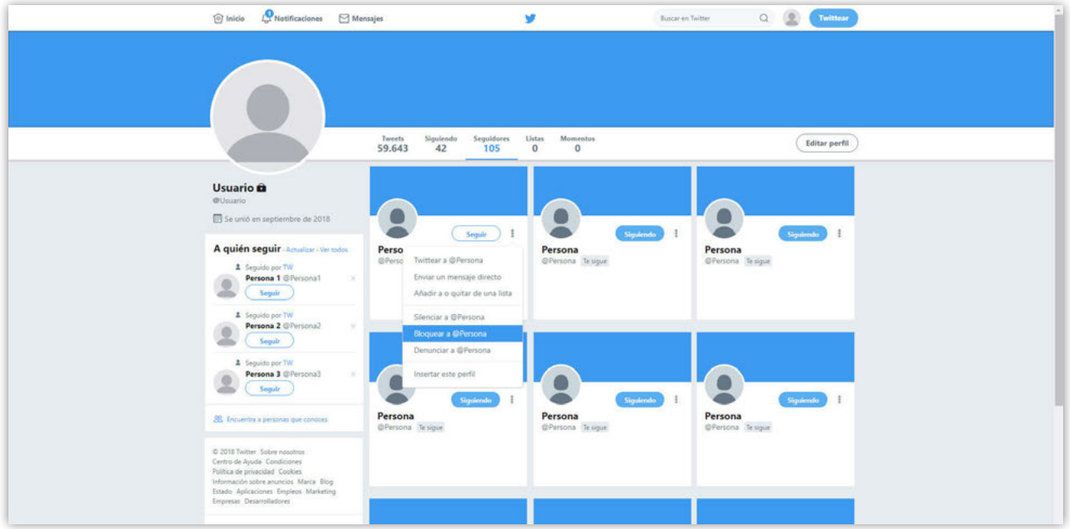
Si tenés configurado tu perfil como “Privado”, para aceptar o rechazar solicitudes de seguidores tenés que acceder a tu perfil y seleccionar la opción “Seguidores”. Si tenés alguna solicitud pendiente, esta se mostrará al lado de todos tus seguidores. Podés aceptar o rechazar la petición. En caso de aceptarla, ese usuario verá tus tuits; de lo contrario, no podrá verlos.



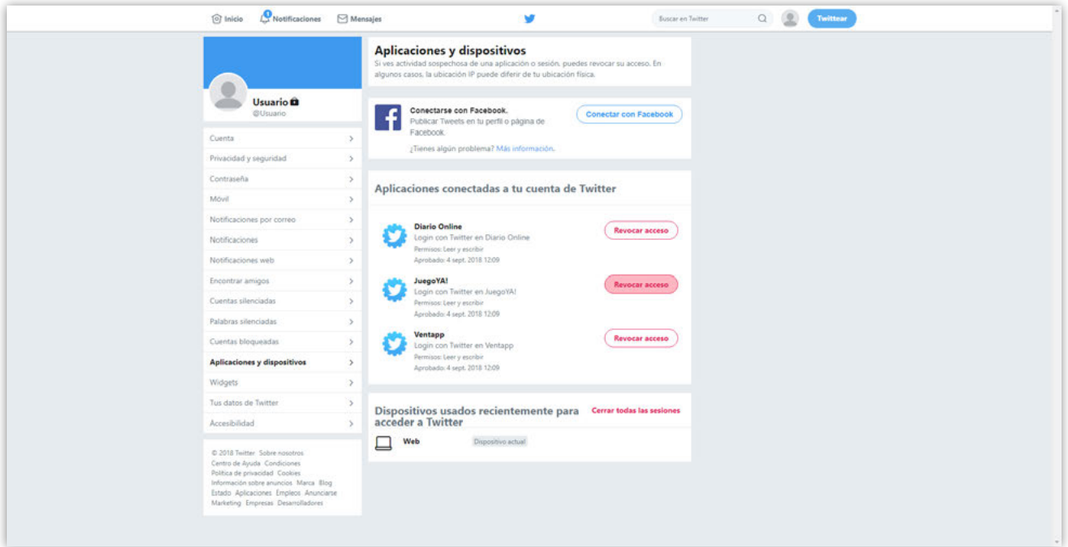
¿Se puede bloquear usuarios?

Si querés silenciar, bloquear o reportar una determinada cuenta de usuario, ya sea porque te está molestando, porque considerás que sus contenidos no son adecuados o simplemente porque no te interesa lo que publica, seleccioná la cuenta en cuestión, desplegá el menú y seleccioná la opción “Bloquear” a determinada persona.





Para finalizar, desde el menú “Aplicaciones” podrás ver todas las aplicaciones que están vinculadas a tu cuenta. Es recomendable que “Revoques el acceso” a todas aquellas aplicaciones que ya no utilices o desconozcas su procedencia y funcionalidad.



6

¿Dónde se puede encontrar más información o realizar consultas y denuncias?

Unidad Reguladora y de Control de Datos Personales (URCDP):

- Dirección: Liniers 1324, piso 4, Montevideo, Uruguay
- Teléfono de consultas: 2901 00 65 opción 3
- Horario de atención: Lunes a viernes de 9:30 a 17:30 horas
- Correo electrónico: infourcdp@datospersonales.gub.uy
- URL: https://datospersonales.gub.uy

Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Cert.uy):

- Dirección: Liniers 1324, piso 3, Montevideo, Uruguay
- Teléfono de consultas: 2 901 29 29, interno 8567
- Horario de atención: Lunes a viernes de 09:30 a 17:30 horas
- Correo electrónico a: cert@cert.uy
- URL: https://www.cert.uy
- Seguridad de la Información - Agesic: seguridad.informacion@agesic.gub.uy
- Campaña de sensibilización Seguro te Conectás: seguroteconectas@cert.uy


ANEP
Educación Pública


CERTuy
CENTRO NACIONAL DE
RESPUESTA A INCIDENTES DE
SEGURIDAD INFORMÁTICA


agesic
DESARROLLANDO
EL URUGUAY DIGITAL


PRESIDENCIA
República Oriental del Uruguay