ENJOY SAFER TECHNOLOGY™

GUÍA DE

Seguridad en redes sociales

Introducción

Las redes sociales son parte de los hábitos cotidianos de muchas personas. Tanto adultos como menores, cualquier internauta usa al menos una red social y la gran mayoría de ellos participan activamente en más de una. Estas plataformas son servicios de Internet que permiten a los usuarios generar un perfil público, en el que pueden plasmar datos personales e información de distinta índole. Tal es el impacto que generaron, que para muchas personas las redes sociales son los motivos principales para conectarse a Internet.

Sin embargo, a partir de su uso constante, los usuarios se ven expuestos a un conjunto de amenazas informáticas que pueden atentar contra su información, privacidad, dinero o incluso su propia integridad.

Ante la creciente tendencia de los ataques informáticos que utilizan las redes sociales como medio para su desarrollo o propagación, se vuelve de vital importancia estar protegido y contar con un entorno seguro al momento de utilizarlas.

¿Cuáles son los principales vectores de ataque a los que se exponen los usuarios de estas redes? ¿De qué manera pueden mejorar los niveles de seguridad? ¿Cuáles son las nuevas problemáticas referidas a la privacidad al subir de manera desmedida distintos contenidos?

Esta guía responderá estas preguntas y mostrará las mejores prácticas para alcanzar una mayor protección mientras se utilizan las redes sociales más populares.

Índice

El alcance de las redes en la actualidad

El alcance de las redes en la actualidad

La selección de redes sociales en las cuales se basa esta guía se debe a su nivel de penetración en distintos países de Latinoamérica y la cantidad de usuarios que las utilizan.

+ 1650 MILLONES DE USUARIOS

Sin lugar a dudas es la mayor red social del mundo.

+ 310 MILLONES DE USUARIOS

Esta aplicación inicialmente pensada para dispositivos móviles, se consolida como el **rey de microbloging**.

+ 1000 MILLONES DE USUARIOS

Principal plataforma utilizada para compartir videos.

+ 400 MILLONES DE USUARIOS

Manipula imágenes en un formato característico y videos de corta duración entre los usuarios de su misma red.

+ 150 MILLONES DE USUARIOS

Híbrido entre una red social y una aplicación de mensajería; debe su fama a su novedosa forma de compartir imágenes que se "autodestruían" luego de cierto tiempo.

+450 MILLONES DE USUARIOS

Basada en contactos profesionales conocidos, los usuarios intercambian distintos tipos de información que van desde búsquedas laborales, hasta opiniones y artículos entre distintos grupos temáticos.

Principales vectores de ataque

Principales vectores de ataque

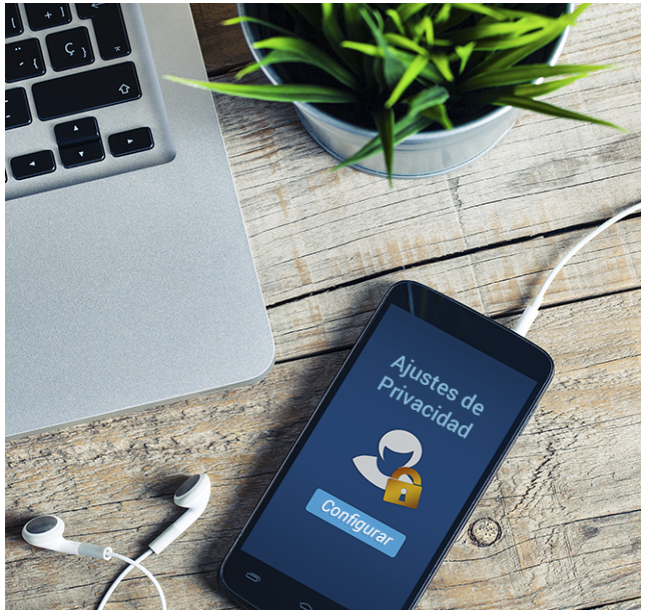
La Ingeniería Social, definido como el arte de disuadir a las personas, es uno de los grandes pilares utilizados por los ciberdelincuentes para llevar a cabo distintitos tipos de ataques. En muchos casos, la información volcada en las redes en conjunto con una **mala configuración de la privacidad** puede ser la fórmula perfecta para generar un señuelo atractivo para la mayor parte de las víctimas. Respecto a los incidentes, la diversidad de ataques puede categorizarse principalmente en seis grandes grupos dependiendo su naturaleza.

Infecciones con malware

Son archivos con fines dañinos que, al infectar una computadora, realizan diversas acciones, como el robo o secuestro de información, el control del sistema, la captura de contraseñas o sesiones activas e inclusive deteriorar el rendimiento del dispositivo infectado. Gusanos, troyanos y ransomware, son las variantes más conocidas en este campo.

Particularmente en Facebook, existieron varias campañas de propagación de malware en las cuales las técnicas de Ingeniería Social fueron el patrón común. **Remtasu**, por ejemplo, se encontraba camuflado en herramientas falsas para tomar el control de cuentas ajenas en Facebook. La campaña de Kilim, por su parte, utilizaba el servicio de mensajería enviando como señuelo un **falso video** el cual finalizaba instalando un complemento en el navegador que comprometía la privacidad de los usuarios. Asimismo, la antigua trampa ligada a **quién visita tu perfil** e inclusive algunas campañas maliciosas que se relacionaban con servicios de mensajería, como **WhatsApp**, también lograron propagarse por esta red social.

La alta efectividad de propagación de este tipo de amenazas, radica en que una vez que la cuenta de la red social es



infectada, los códigos maliciosos la aprovechan para continuar esparciéndose entre los contactos de la víctima.

Estafas digitales

Al igual que determinados códigos maliciosos, las estafas digitales también se propagan en redes sociales. Particularmente a través de Facebook, se vieron casos de engaños vinculados a servicios de SMS Premium.

Por otra parte, los incidentes de **phishing** siguen siendo una de las principales preocupaciones. A través de un correo apócrifo, los ciberdelincuentes se hacen pasar por una entidad conocida e invitan al receptor de la estafa a acceder a un enlace. Cuando la víctima lo hace parece estar en el sitio real, sin embargo, el dominio que está visitando no pertenece a

la entidad conocida y su única función será capturar su nombre de usuario y contraseña. De esta manera, los ciberdelincuentes se hacen con credenciales de acceso de muchas cuentas de redes sociales e, inclusive, entidades financieras.

¿Cómo reconocer un correo de phishing, un falso enlace o un sitio apócrifo?

Normalmente estos correos llegan encabezados por un usuario genérico como por ejemplo el clásico "Estimado usuario"; otra característica muy común es que al posicionar el cursor sobre el enlace, aparecerá una nueva dirección que difiere del enlace que aparece a simple vista. Por último, se debe verificar que la URL comience con el protocolo HTTPS, dado que ofrecerá más seguridad al cifrar la comunicación con el sitio.

Robo de información

En el uso diario de las redes sociales, los usuarios comparten diversos datos de índole personal que pueden ser de utilidad para los atacantes. El robo de información en redes sociales se relaciona directamente con el robo de identidad, uno de los delitos informáticos que más ha crecido en los últimos años.

Los dos vectores de ataque más importantes para el robo de información son:

Ingeniería Social

Se busca el contacto directo con la víctima, extrayendo información a través del vínculo, la "amistad" o cualquier comunicación que permita la red social.

Información pública

Una mala configuración de las redes sociales puede permitir que información de índole personal esté accesible más allá de lo que el usuario desearía o le sería conveniente. Los cibercriminales buscan este tipo de descuidos para hacerse con dicha información.

Grooming

Consiste en acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad y abusar sexualmente de él. Las redes sociales son un espacio en donde este tipo de riesgos está muy latente, puesto que los groomers pueden aprovecharse del anonimato para hacerse pasar por niños y, así, llegar a sus víctimas.

Si bien es cierto que lo menores aprenden con mayor velocidad y están al día con las nuevas aplicaciones y tecnologías, ellos no perciben con la misma naturalidad la maldad o segundas intenciones que puede tener un adulto desconocido quien, en muchos casos, esconde su identidad.

+ VER LA GUÍA DE PROTECCIÓN INFANTIL

Si bien es cierto que lo menores aprenden con mayor velocidad y están al día con las nuevas aplicaciones y tecnologías, ellos no perciben con la misma naturalidad la maldad o segundas intenciones que puede tener un adulto desconocido quien, en muchos casos, esconde su identidad.

Cyberbulling

Implica la utilización de medios de comunicación digitales, como las redes sociales, sitios webs, foros, etc., con el fin de acosar y hostigar de forma premeditada a una persona o grupo. El cyberbulling se expande viralmente por la Web y puede ser difícil de detener; por tal motivo, resulta invasivo y dañino.

Las formas más comunes son la difusión de falsos rumores, videos o fotos humillantes, y la creación de perfiles o sitios para agredir a la víctima. También puede ocurrir que el agresor se haga pasar por otra persona para decir cosas desagradables o amenace a la víctima con publicar su información personal.

Las formas más comunes son la difusión de falsos rumores, videos o fotos humillantes, y la creación de perfiles o sitios para agredir a la víctima. También puede ocurrir que el agresor se haga pasar por otra persona para decir cosas desagradables o amenace a la víctima con publicar su información personal.

+ VER VIDEO DE CYBERBULLYING

Sexting

Consiste en el envío de contenidos de tipo sexual, principalmente fotografías y/o vídeos, a otras personas por medios digitales.

Una de las redes sociales más afectadas con esta problemática es Snapchat, la cual permite el envió de este tipo de contenido con la ilusión de que esta información se borrará a los pocos segundos. Ahora bien, si este contenido cae en las manos equivocadas se viraliza extremadamente rápido, es decir que se difunde masivamente sin ningún tipo de control en las redes causando un gran impacto social en los actores involucrados.

Prácticas para lograr un mayor nivel de seguridad

Prácticas para lograr un mayor nivel de seguridad

Ante este escenario de amenazas, el uso de redes sociales puede parecer peligroso. No obstante, si se siguen ciertos consejos y buenas prácticas, es posible utilizarlas y contar con niveles de protección adecuados para un uso correcto y seguro de estas plataformas.

Como principales medidas se destacan: utilizar soluciones de seguridad, configurar correctamente los usuarios en las redes sociales, utilizar cuando de sea posible un segundo factor de autentificación y el protocolo HTTPS para la navegación.

No obstante, la constante educación y el uso cuidadoso al momento de la navegación, siempre permitirán minimizar de forma importante los riesgos.

Soluciones de seguridad

Siendo los códigos maliciosos la amenaza masiva más importante, la utilización de un software antivirus con capacidades proactivas de detección y con una base de firmas actualizadas, es un componente fundamental para prevenir el malware que se propaga por redes sociales.

Las herramientas de antispam y firewall también permiten optimizar la seguridad del sistema ante estos riesgos. También es fundamental no utilizar un usuario con permisos de administrador al momento de navegar por estas redes, y que cada persona que use el equipo tenga sus propios perfiles. Esta es una forma de minimizar el impacto en caso que ocurra un incidente.

Finalmente, para monitorear y supervisar el uso por parte de los menores de edad, existen herramientas de control parental que permiten bloquear sitios web indeseados, así como también restringir ciertas franjas horarias (como cuando el niño está en la escuela, por ejemplo) o, de plano, la cantidad de tiempo en que el niño utiliza las redes sociales.

Contraseñas

Las contraseñas son la llave de tu identidad digital, por esto es sumamente importante que las cuides. Puedes utilizar las recomendaciones que siguen para proteger tus cuentas de redes sociales:

- No uses tu contraseña de una red social en otros sitios de internet y nunca la compartas.
- Evita incluir tu nombre o palabras comunes. La contraseña debe ser difícil de adivinar.
- Evita utilizar computadoras públicas para ingresar en redes sociales. Recuerda cerrar sesión, sobre todo cuando utilices una computadora que compartas con otras personas.
- Piensa dos veces antes de hacer clic o descargar cualquier contenido, recuerda que puede ser algún señuelo de Ingeniería social.

Configuraciones

Por defecto, no siempre las configuraciones en las redes sociales son las más óptimas para tu seguridad. Por lo tanto, es recomendable dedicar un tiempo prudencial al momento de registrarse, además de revisar cuáles son las posibles fugas de información ante una mala configuración del sistema en cuanto a la **privacidad**.

De ser posible, para una mayor seguridad en tu cuenta es recomendable configurar un segundo factor de autentificación; si no estás familiarizado con esta metodología, puedes echar un vistazo a la **guía de doble autentificación**.

A continuación, se detallan las principales recomendaciones en las redes sociales mayormente utilizadas.

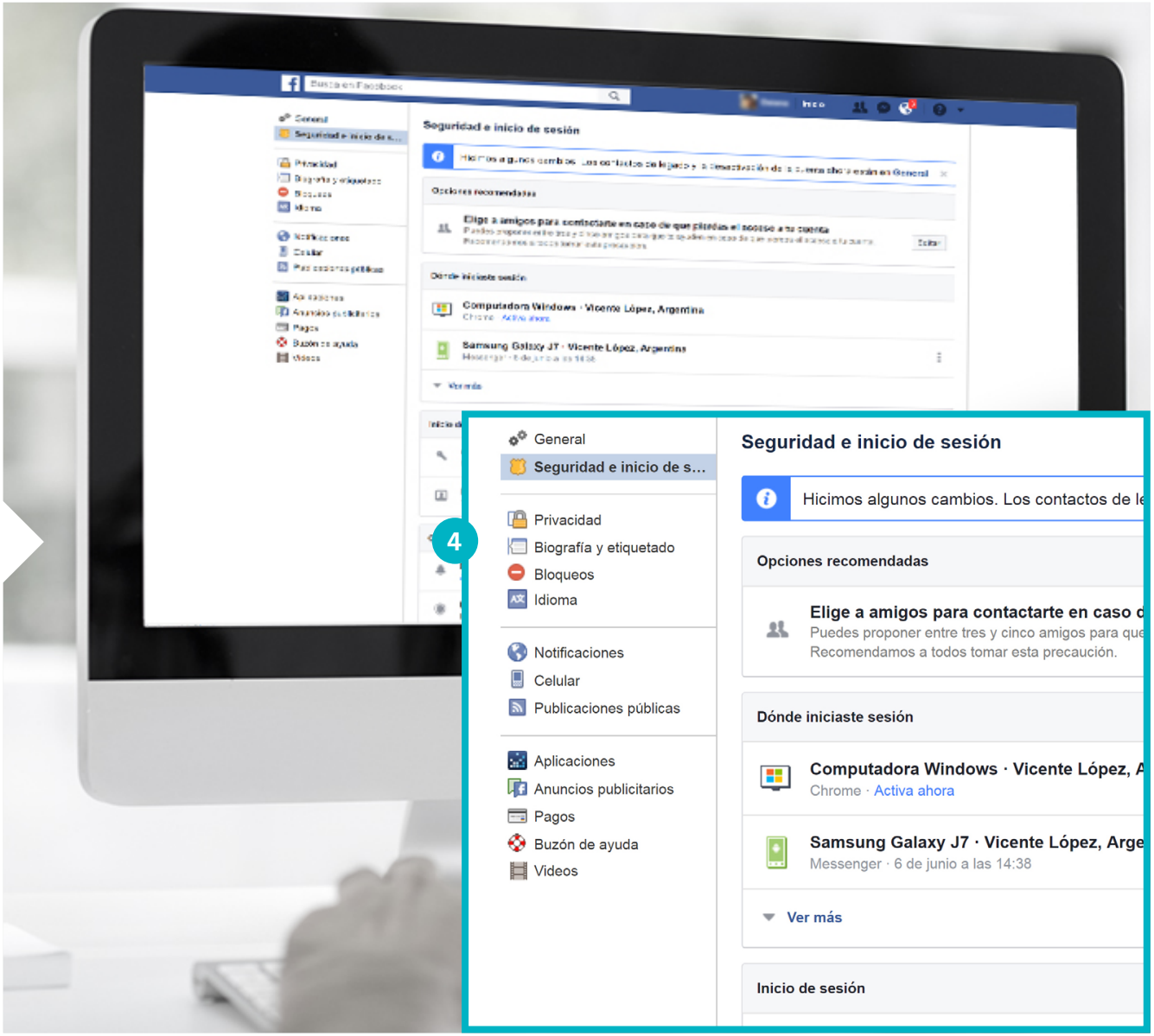
Facebook

Para analizar el estado de la configuración en esta red social se deben hacer simplemente tres clics, comenzando en el la flechita superior derecha **(ref. 1)** , para luego entrar en configuración **(ref. 2)** y, por último, en seguridad y privacidad **(ref. 3)**, como podrás visualizar en las imágenes.

Una vez dentro de Seguridad, se podrán configurar valores los cuales tendrán un mayor o menor impacto en la seguridad de las cuenta, es recomendable que te familiarices con estos.

Es importante activar las opciones de alertas y aprobaciones de inicio de sesión. Si tienes algún tipo de inquietud sobre si otra persona está ingresando a tu perfil, puedes revisar las opciones de "navegadores de confianza" **(ref. 4)** y "dónde iniciaste sesión".

Por otra parte, controlar la privacidad será de mayor relevancia para elevar el grado de protección sobre tu perfil.



Estas son algunas opciones con las cuales conseguirás limitar la masificación de tu información. Como puedes ver en la imagen, Facebook principalmente basa su privacidad desde tres pilares: quién puede ver tus contenidos **(ref. 5)**, quién puede ponerse en contacto **(ref. 6)** y quién puede buscarte **(ref. 7)**.

En cuanto a quién puede ver tus publicaciones, es recomendable la opción "Solo yo", ya que luego de revisar una publicación podrás cambiar el estado a "amigos". De este modo, protegerás tu privacidad en caso de publicar algo por error.

Respecto a quién puede buscarte, es aconsejable evitar que los motores de búsqueda enlacen tu perfil, de este modo tus fotos publicadas no serán vistas ni encontradas simplemente con una petición en Google.

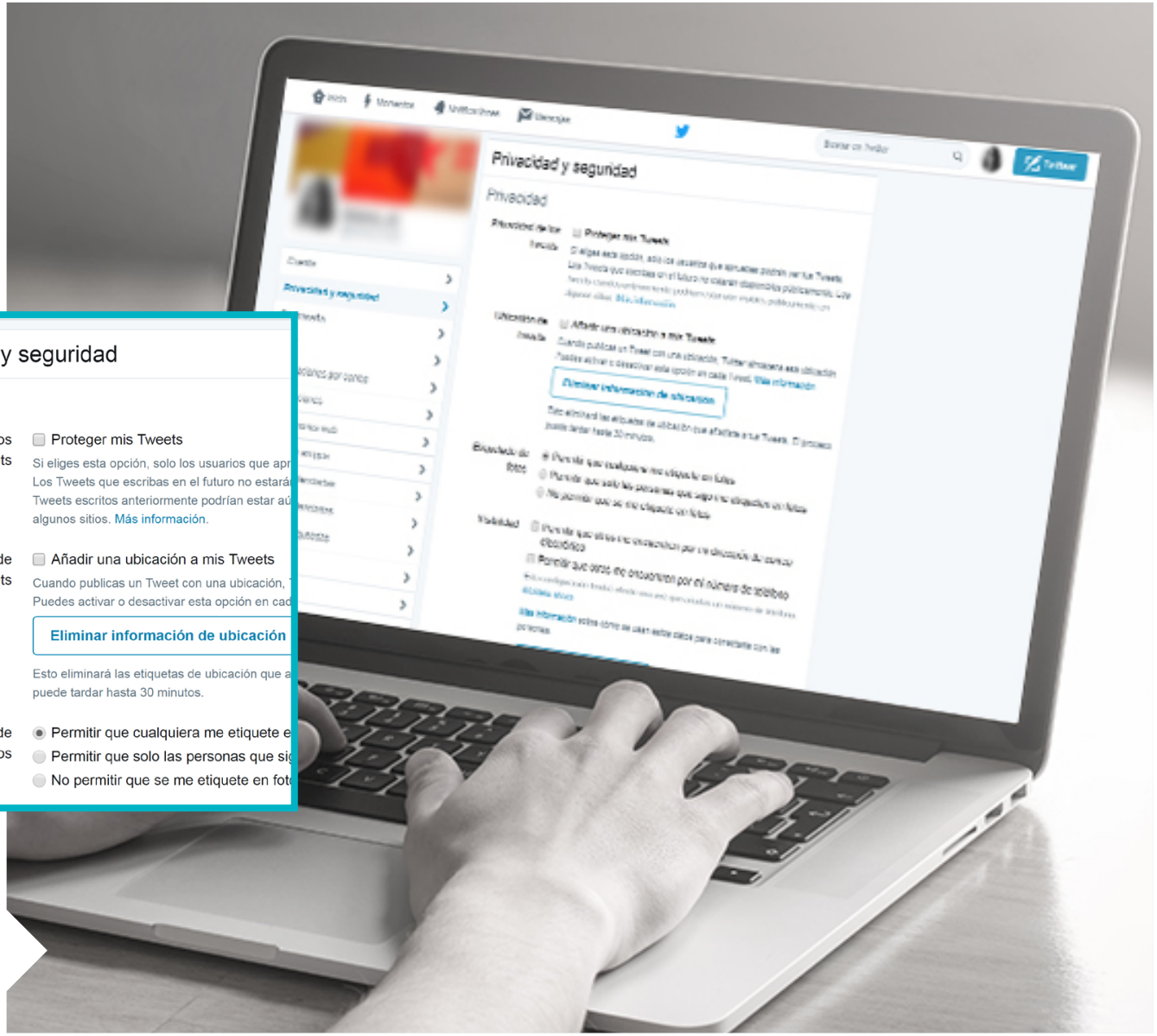
Desde luego, no hay que agregar gente que no sea conocida, y por supuesto si eres menor de 13 años no deberías usar esta red social.

Twitter

Para revisar la configuración de seguridad de tu perfil en esta red social, deberás hacer clic en tu imagen en el margen superior derecho **(ref. 1)**, luego en "configuración y privacidad" **(ref. 2)** y luego en "Móvil" **(ref. 3)**.

Para reforzar la seguridad, podrás activar la opción de verificación de sesión **(ref. 4)**, la cual enviará un SMS con un código al teléfono móvil, el cual se te pedirá para comenzar a utilizar Twitter. De esta manera, en caso de que te roben la contraseña no podrán ingresar a tu cuenta.

Ademas, es muy importante que cuides tu privacidad **(ref. 5)**, por lo tanto no deberías dejar que otras personas pueda etiquetarte en su foto. Por otra parte, si eliges la opción de "Proteger tus tweets", tus publicaciones solo serán vistas por los perfiles de personas que tú autorices. Por último, desactivando la pestaña de añadir ubicación, estarás preservando en mayor medida tu sobreexposicion en esta red.



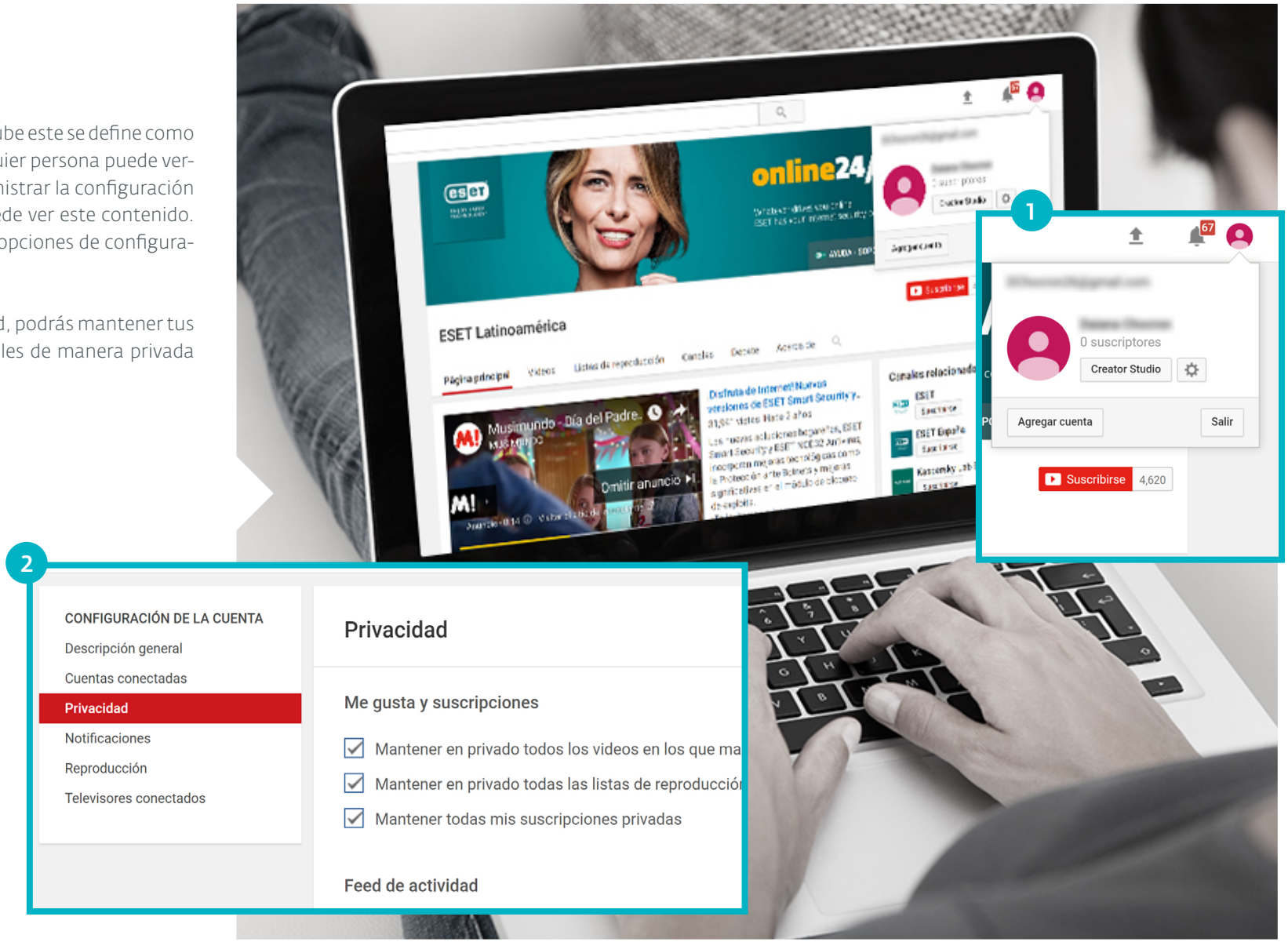
Instagram

Esta aplicación es utilizada para compartir imágenes y videos de corta duración. Por lo tanto, las medidas de seguridad están aplicadas a quién puede ver los contenidos publicados. En la siguiente imagen, podrás ver cómo configurar el perfil en modo "cuenta privada". De esta manera, cuando alguien desconocido quiera visualizar tu contenido deberá enviarte una petición.

Youtube

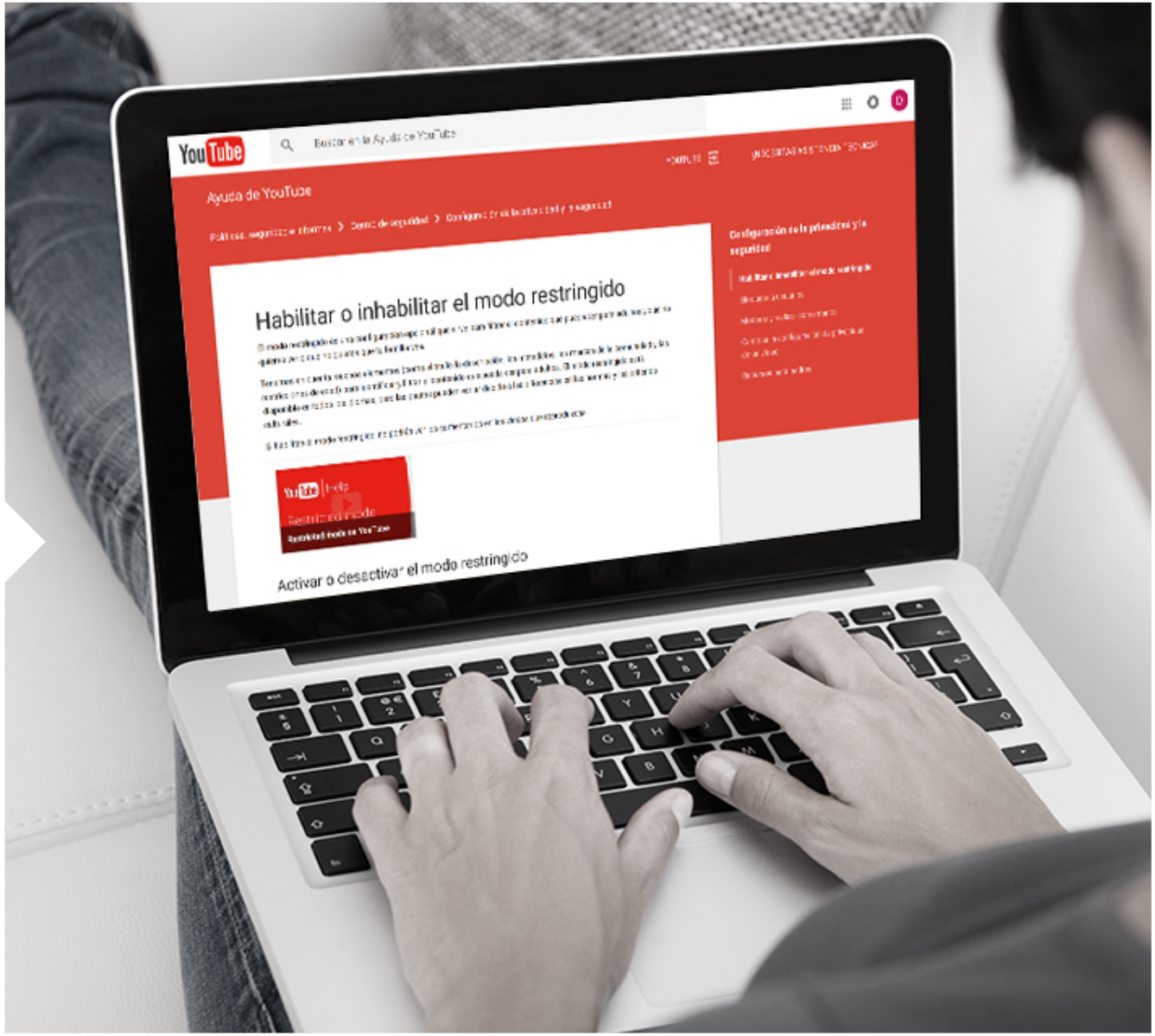
Por defecto, al subir un video a YouTube este se define como "público", lo que significa que cualquier persona puede verlo. En este sentido, es posible administrar la configuración de privacidad y controlar quién puede ver este contenido. Para hacerlo, debes ingresar en las opciones de configuración de tu cuenta **(ref. 1)**.

Ingresando en el menú de privacidad, podrás mantener tus videos y suscripciones a otros canales de manera privada **(ref. 2)**.



Además, podrás habilitar el **modo restringido**, que es una configuración que permite descartar contenido potencialmente indeseable que preferirías no ver o con el que no querrías que se encontraran menores de edad o miembros de tu familia. En otras palabras, es una especie de control parental específicamente para YouTube.

Tanto esta opción como otras interesantes que deberías observar, las podrás encontrar en el **Centro de seguridad** de la plataforma.

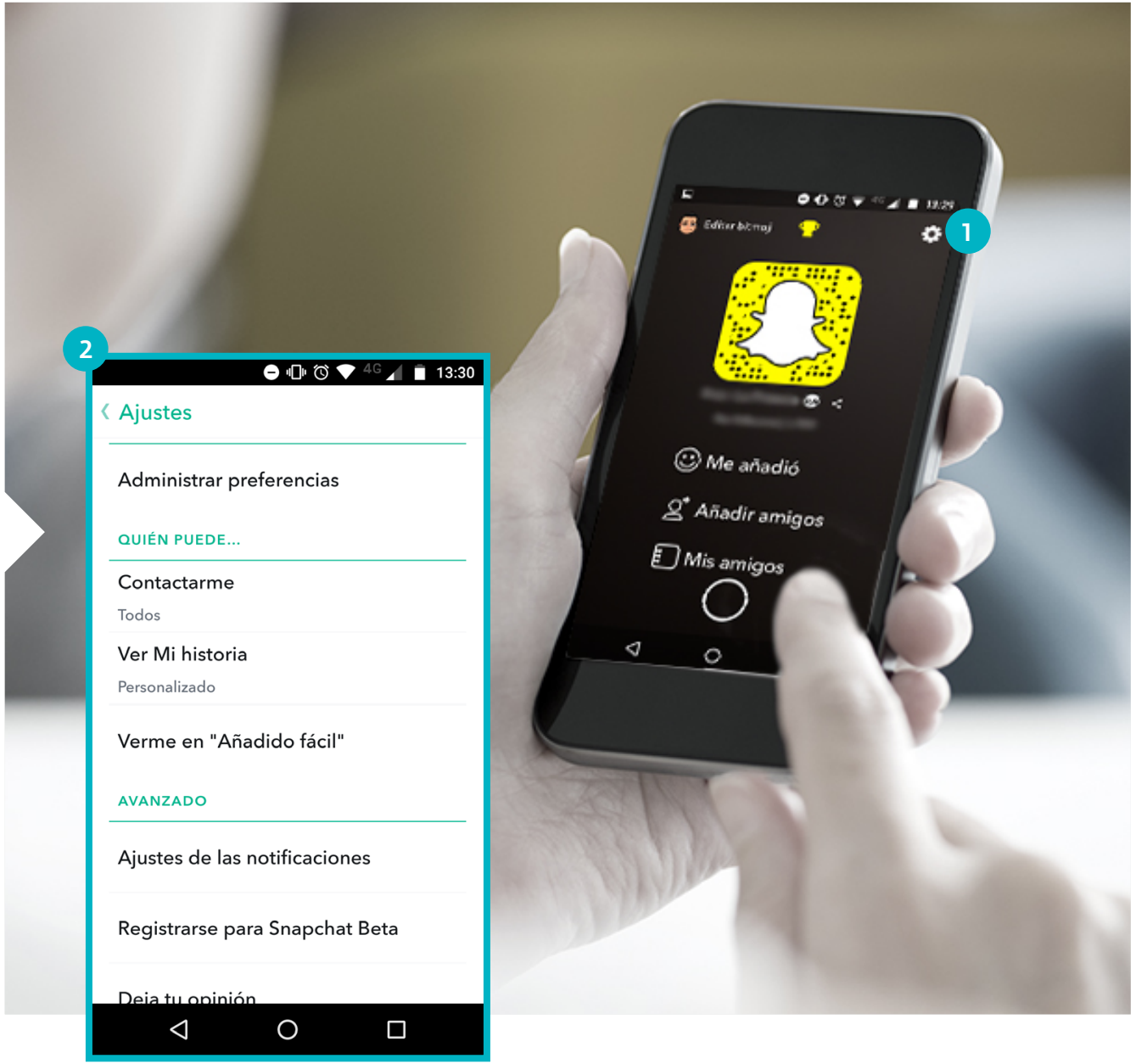


Snapchat

Un consejo importante referido al uso de esta aplicación es que no debes olvidar de que cualquiera puede tomar una captura de pantalla de un snap o simplemente usar otra cámara para tomarle una foto. Por este motivo, es aconsejable no enviar material que pueda ser utilizado para hostigarte a ti o a otra persona.

Por otra parte, deslizando la pantalla hacia abajo aparecerá una nueva interfaz desde donde podrás configurar tus ajustes de seguridad. Solo debes hacer clic en el extremo superior derecho, tal como se ve en la imagen **(ref. 1)**

Dentro del menú de ajustes, podrás configurar opciones de privacidad relacionadas a quién puede contactarte y ver tu historia **(ref. 2)**.



Conclusión

Sin lugar a dudas, las redes sociales son un valioso recurso para los usuarios. Desde aportes en educación, hasta las interrelaciones de grupos mixtos, dejan en claro que estas redes pueden ser utilizadas con fines benignos. Si bien esto forma parte de la interacción social normal que se da en la actualidad, es necesario considerar que Internet es un mundo digital expuesto, es decir que cualquier acción que se haga puede tener un impacto global y permanente.

También resulta peligroso publicar datos que puedan identificar a una persona como dirección, teléfonos, lugar de estudio o trabajo, días de vacaciones, etc. Esto puede resultar todavía más complicado si se posee una gran lista de amigos que no son conocidos personalmente.

Asimismo, existen una serie de amenazas que pueden comprometer a adultos y menores durante el uso de las mismas. Por este motivo, es recomendable no subestimar el valor de la privacidad y seguridad en la redes, así como tampoco a los delincuentes informáticos. De este modo, se debe hacer un buen uso de herramientas tecnológicas, tener configuraciones correctas, además de una conducta adecuada durante la navegación y publicación de contenidos.

De esta forma, más allá del perfil del usuario y la naturaleza de sus contenidos compartidos, será posible disfrutar de las tecnologías y las redes sociales de una forma segura.

www.eset-la.com

/esetla

@esetla

/company/eset-latinoamerica