MANUAL DE MUJERES CIBERSEGURAS

Instituto Municipal de la Mujer de Aguascalientes

Aguascalientes
LA CIUDAD DE TU VIDA

Comisario Gral. Mtro. en D. C. y A. Antonio Martínez Romo Secretario de Seguridad Pública Municipal de Ags

El principal objetivo es brindar las medidas de seguridad en las redes sociales más utilizadas por adolescentes y adultos, buscando fortalecer en la sociedad la ciberprevención, considerando además la cibervictimización que actualmente sufren las mujeres de diversas edades en dichas redes sociales.

Lic. Zayra Angélica Rosales Tirado Directora General del Instituto Municipal de la Mujer de Aguascalientes

Con gran compromiso, para tí, mujer que busca desarrollarse en todas las esferas sociales, entre ellas la cibernética, te comparto este Manual para ayudarte a fortalecer tu ciberseguridad en tus redes sociales y así fortalecer la cultura de alfabetización digital.

Guía de Teléfonos de Emergencia

• **C4 Municipal**	(449)994.6600
• **Unidad de Inteligencia Cibernética**	(449)390.3281
• **Casa Rosa VNSA**	(449)251.3213 (449)251.699
• **Casa Rosa VNSA WhatsApp**	(449)365.5861
• **Casa Rosa Insurgentes**	(449)978.9592
• **IMMA Centro**	(449)916.3610
• **Delegación Insurgentes**	(449)978.1170
• **Delegación Pocitos**	(449)999.6375
• **Delegación Terán Norte**	(449)993.7443
• **Delegación Terán Sur**	(449)972.6842
• **Delegación Centro**	(449)993.0045

Lenguaje mayormente usado por adolescentes en mensajes de texto

Significado de términos o abreviaturas que los padres de familia deben conocer.

- **1174:** Lugar de encuentro para una fiesta.
- **53X:** Sexo (Sex) deletreado con número.
- **AF:** Usado para enfatizar emociones o calificativos, por ejemplo: “Exited AF”.
- **Bae:** Es un termino afectuoso, que se usa en parejas o a la persona que le gustas.
- **Cook session:** Término que se describe como el ciberbullyng.
- **CU46:** Abreviación de “See you for sex” o nos vemos para tener sexo.
- **Dox:** Cuando se revela la información personal de una persona, por ejemplo: “la porno venganza”.
- **GNOC:** “Get naked on camera” ó “desnúdate en frente a la cámara”.
- **GPI:** Gracias por invitar.
- **POV:** Punto de vista desde primera persona.

- **Dddd:** Se utiliza para algo que se dice con ironía o sarcasmo.
- **NTP:** No te preocupes.
- **NTC:** No te creas.
- **ALV:** A la versh.
- **BAE:** Antes que nadie.
- **NPI:** Ni pinche idea o ni p*ta idea.
- **CHTM:** Abreviatura para mentar la madre.
- **F:** Tristeza y respeto.
- **TP:** Te publico.
- **TC:** Te comento.
- **HDP:** Hijo de p*ta.
- **HDTPM:** Hijo de tu puta madre.
- **ABC:** Ando bien cachondo.
- **WA:** Te escribo por WhatsApp.
- **VPG:** Vamos por unas caguamas.

- **GOAT:** “Greatest Of All Time” o el mejor de todos los tiempos.

- **ILY:** “I Love You” o “Te Amo”.

- **IWSN:** I want sex now” o Quiero Sexo Ahora”.

- **LMAO:** Es una forma burlona de decir me estoy riendo mucho .

- **NIFOC:** Estoy desnudo frente a la computadora.

- **PIR:** “Padre en el cuarto”. Para advertir a la persona que tenga cuidado con lo que dice y hace, ya que lo están vigilando.

- **POS:** “Parent over shoulder”. Advertencia de que alguno de sus padres esta presente viendo su dispositivo.

- **Shipping**: Una forma de decir relación, como decir a una persona que deberían comenzar a tener una relación amorosa.

- **Snapped:** Se usa para describir el enviar un video o foto dentro de una red social.

- **Vamping:** Se refiere a quedarse despierto toda la noche usando redes sociales o en linea. Ya que es la hora en que nadie los puede vigilar.

- **YOLO:** Solo se vive una vez o vivir el momento. Se relaciona con el disfrute de la vida.

Glosario Cibernético

- **Según la Secretaria de las Mujeres:** La violencia digital contra las mujeres y niñas mediante las redes sociales (también conocida como ciberviolencia), puede tener diversas manifestaciones como el ciberbullying, el sexting, el stlaked, el grooming, el shaming y el doxing, algunos otros ejemplos son la difusión, sin el consentimiento de la víctima, de sus datos e imágenes personales, amenazas, difamaciones, acoso, humillación, ataques que afectan la li-bertad de expresión de las mujeres.

- **Ciberbullying:** Es un término que se utiliza para describir cuando una persona es molestada, ame-nazada, acosada, humillada, avergonzada o abusada por otro, a través de Internet o cualquier medio de comunicación como teléfonos móviles o tablets, pue-de ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juego, en general en cualquiera de las tecnologías digitales.

- **Grooming:** Se refiere a un adulto que pretende generar un vinculo de confianza con un menor de edad mediante el uso de un perfil en redes sociales donde se muestra como un menor de edad para diferentes fines, entre ellos el generar material de abuso sexual infantil, secuestro, trata de personas, prostitución, violación, entre otros.

- **Violación a la intimidad personal:** Se refiere a divulgar, compartir, distribuir, comercializar, almacenar, ofertar, publicar o amenazar con publicar por cualquier medio, imágenes, audios o audios de contenido real, manipulado y/o alterado de una personal desnuda total o parcialmente, referente al pene, senos, glúteos o la vagina, o bien actos sexuales o eróticos, ya sea impreso, grabado o digital, sin consentimiento de quien sufre la afectación.

- **Sexting:** Compuesto por “sex” sexo y “testing” escribir mensaje, consiste en el envío de imágenes, videos, audios y mensajes de contenido sexual/ erótico mediante el uso de dispositivos tecnológicos, utilizando redes sociales, plataformas de comunicación y entretenimiento.

- **Ciberacoso:** Se refiere al asedio constante que se genera mediante el uso de plataformas de mensajería, entretenimiento, entre ellas destaca el uso de redes sociales.

- **Doxing:** El término proviene de la frase en inglés dropping docs y consiste en la extracción y la publicación no autorizadas de información personal como el nombre completo, la dirección, números de teléfono, correos electrónicos, el nombre del cónyuge, familiares e hijos, detalles financieros o laborales.

- **Suplantación de identidad:** actividad malintencionada que busca hacerse pasar por otra persona o entidad por diferentes motivos: robo de datos, fraudes y engaños para obtener información o un beneficio económico, ciberacoso, extorsión, grooming, etc.

- **Fraude cibernético:** engaño o estafa pero que es llevado a cabo a través de internet.

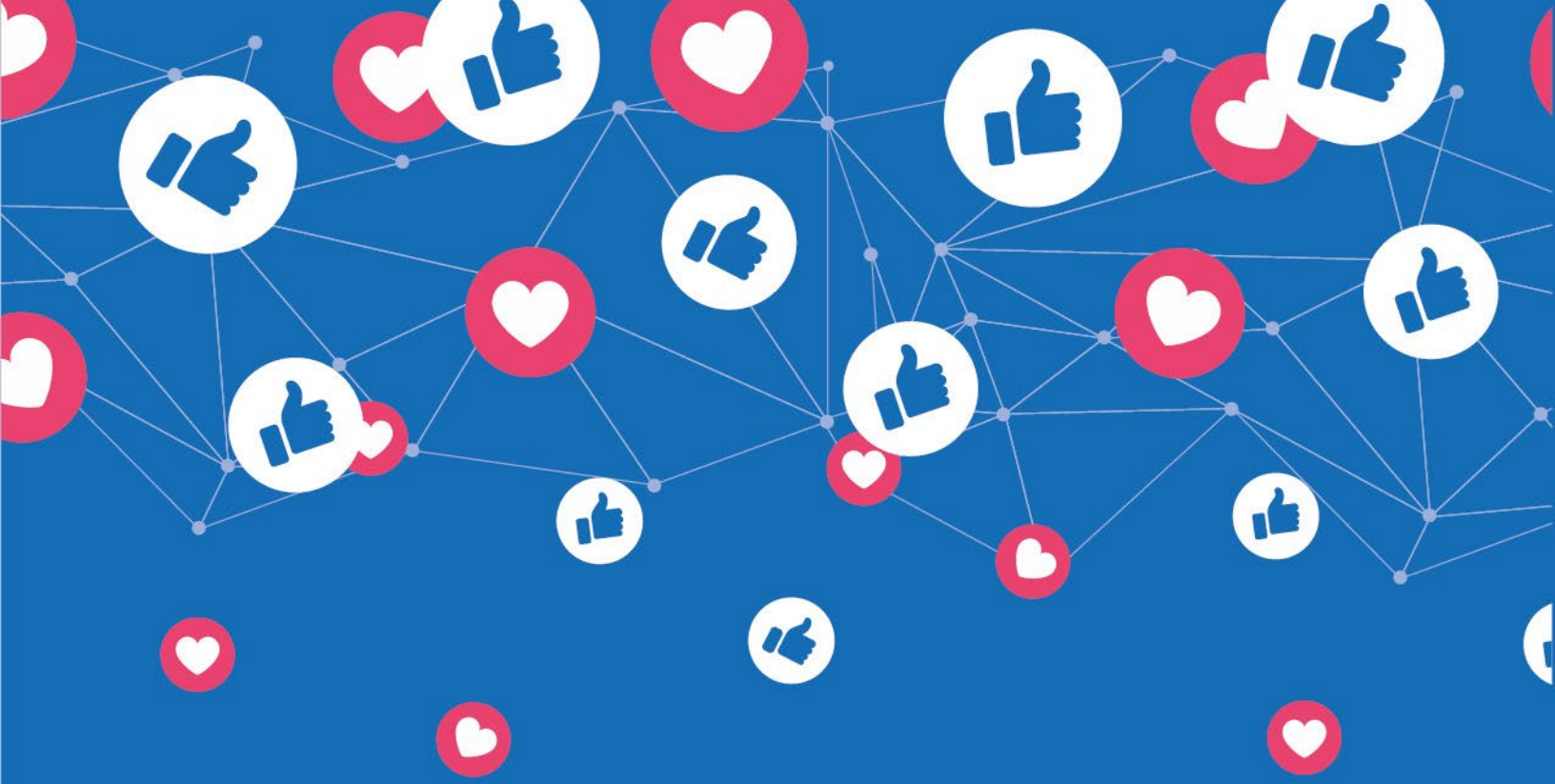
- **Phishing:** El phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial.

- **Vishing:** Forma de timo en la que los delincuentes intentan engañar a la víctima a través de una llamada telefónica, suplantando la identidad de otra persona o, como en el anterior ejemplo, de una organización como una entidad bancaria. También puede ser de una empresa de energía, de gas o de cualquier otra que les sirva como excusa para establecer una comunicación.

- **Smishing:** Técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima red social, banco, institución pública, etc. con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto.

- **Pharming:** combinación de los términos “phishing” y “farming”, es un tipo de cibercrimen muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial.

- **Redes sociales:** tipo de social media centrado en conectar personas entre sí. Cada usuario crea su perfil e interactúa con otras personas compartiendo información. Los individuos no necesariamente se tienen que conocer antes de entrar en contacto a través de una red social, sino que pueden hacerlo a través de ella.



facebook

Red social con alcance a nivel mundial.
interconecta a más de **1000,000,000** usuarios.
Forma parte del “Metaverso” junto a Instagram y WhatsApp.

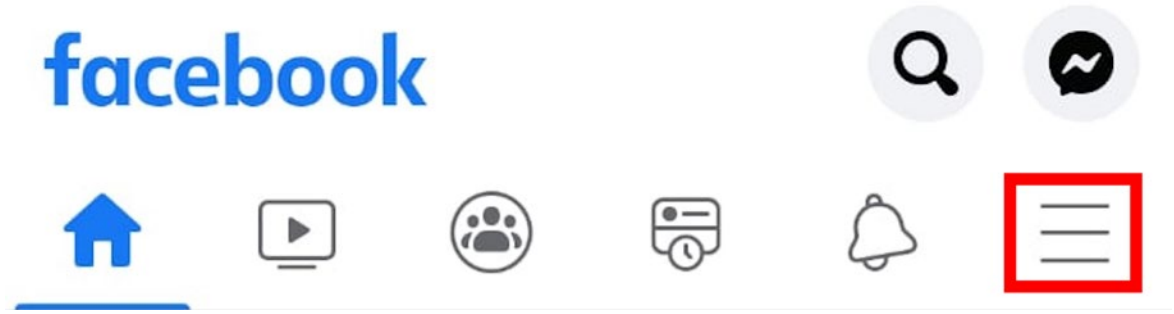
Consejos de seguridad en Facebook

- Evita publicar tus datos personales.
- Evita compartir tu ubicación en tiempo real.
- No publiques fotografías en las que aparezca el exterior de tu casa o las placas de tu coche.
- No aceptes solicitudes de desconocidos.
- No olvides que lo que publicas en tus redes es lo que permites que otros conozcan sobre ti.

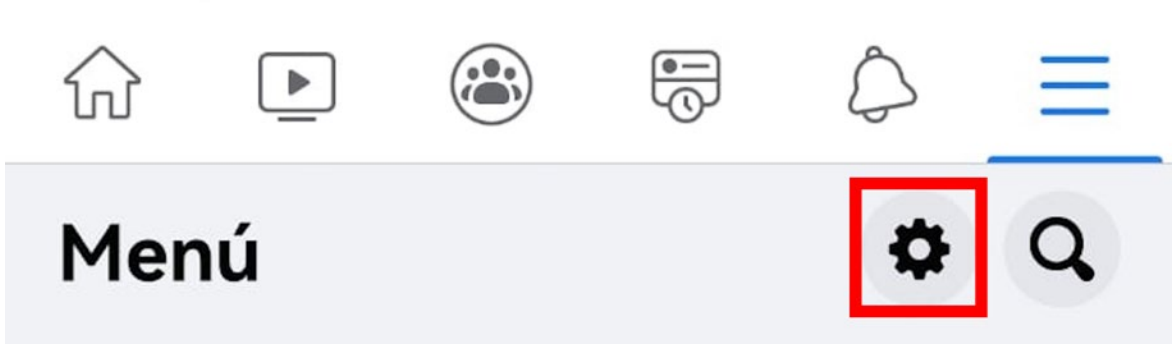
Configuración de seguridad

Es importante blindar nuestro perfil de Facebook con el fin de evitar convertirnos en víctimas de algún delito cibernético.

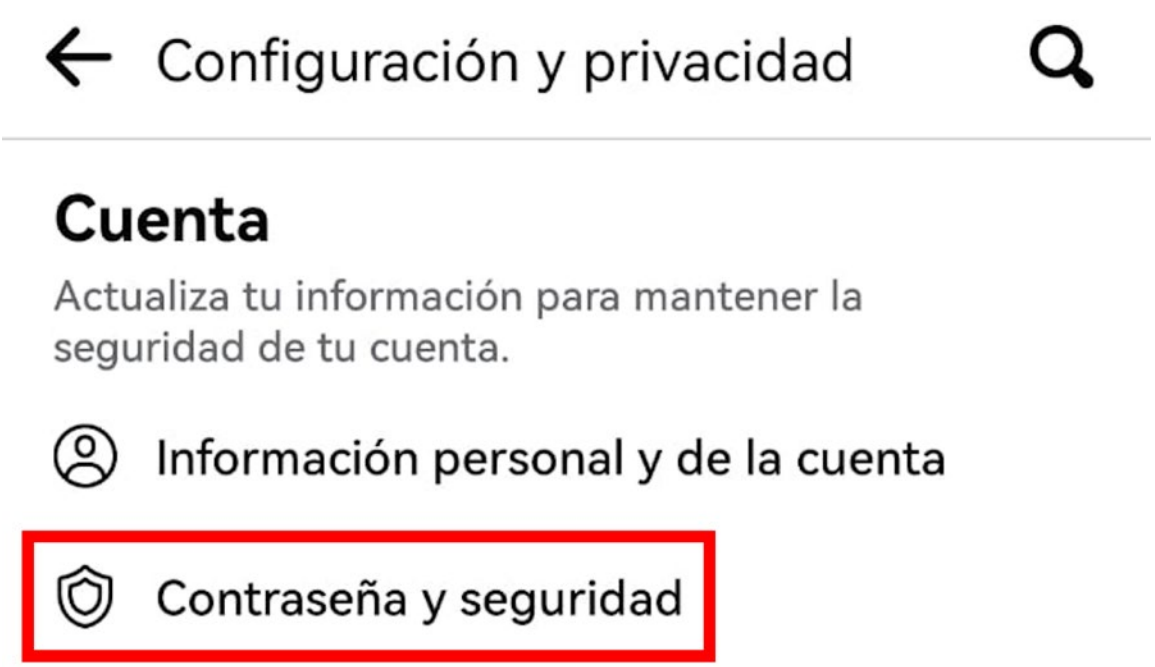
1


facebook

2

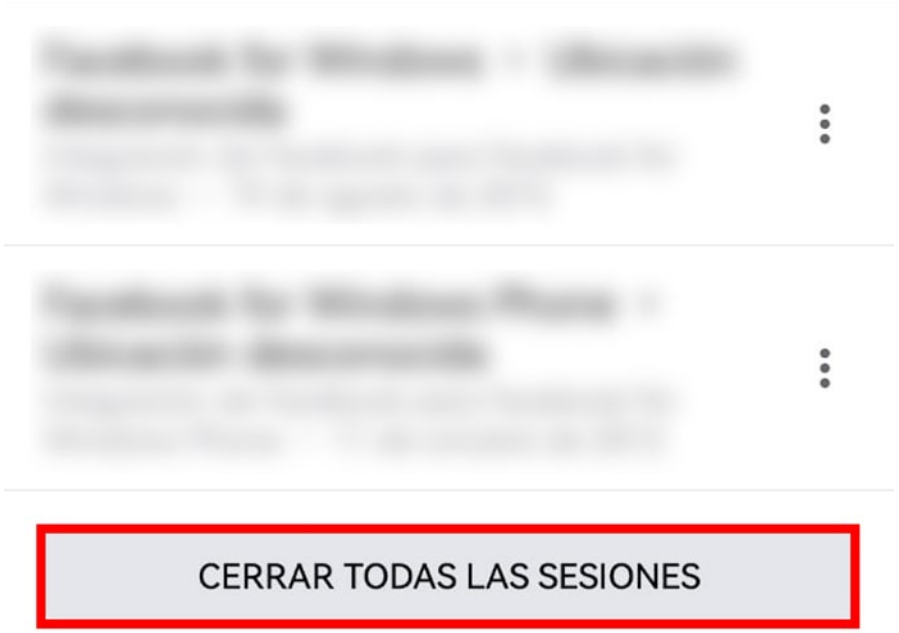

Menú

3


Configuración y privacidad
Cuenta
Actualiza tu información para mantener la seguridad de tu cuenta.
Información personal y de la cuenta
Contraseña y seguridad

4

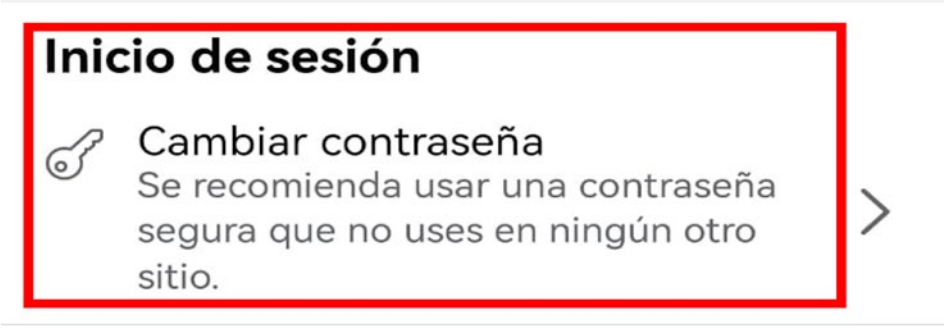
5



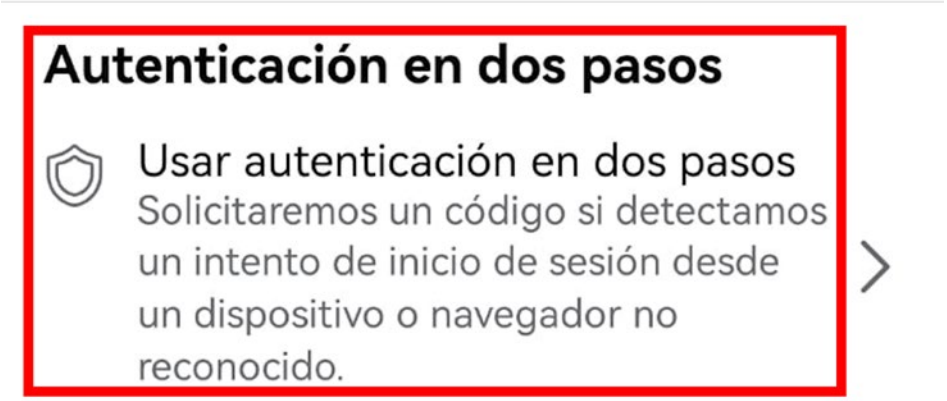
De este modo podrás comprobar si hay algún inicio de sesión que no hayas realizado tú y de esta manera cerrarla inmediatamente.

Es importante tener en cuenta las siguientes medidas de seguridad. Estos pasos se desglozan en el menú anterior.

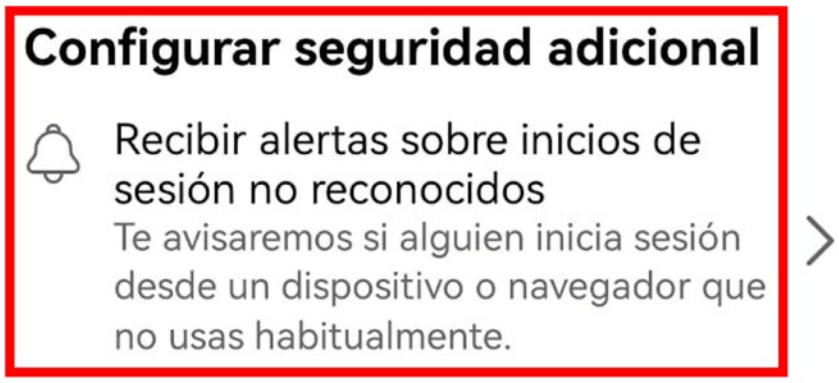
Es recomendable realizar un cambio de contraseña cada mes.



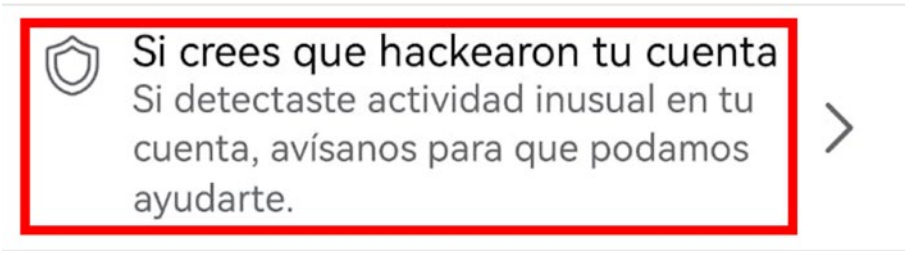
La verificación en dos pasos es una medida de protección de doble capa, para evitar el robo de tu cuenta.



Al activar esta opción, cada que un tercero trate de iniciar sesión, le será notificado.



Con ésta opción puede descartar cualquier vulnerabilidad o riesgo en la cuenta.



Aplicación móvil gratuita que permite la subida de imágenes y videos a través de un perfil personal (y ahora también profesional).
IG nació en 2010 siendo diferente a todas las demás redes sociales puesto que sólo se pueden subir imágenes a través de la aplicación móvil.

Consejos de seguridad en Instagram

- Evita publicar tus datos personales.
- No publiques fotografías en las que aparezca el exterior de tu casa o las placas de tu coche.
- No aceptes solicitudes de desconocidos.
- No olvides que lo que publicas en tus redes es lo que permites que otros conozcan sobre ti.

Contraseña segura

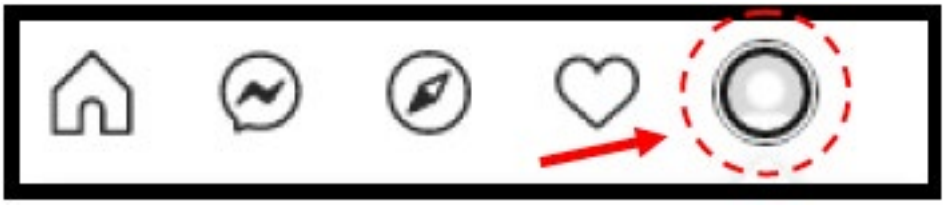
- Para que una contraseña sea segura, es importante que cuente con 10 dígitos, así como la combinación de letras, números y caracteres especiales.
- Evita repetir contraseñas entre aplicaciones.
- Cambia tus contraseñas cada 3 meses.

- Evita compartir tus contraseñas.
- Aplica verificación en dos pasos.

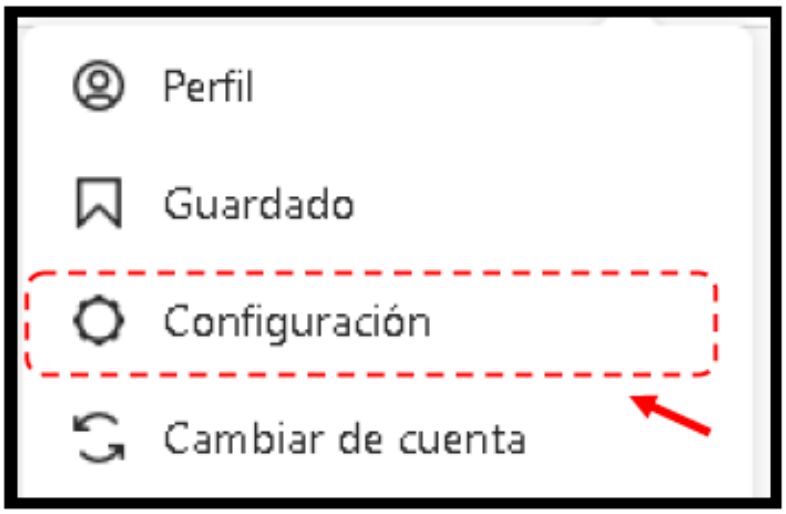
NZ!aT3_$94

12345678

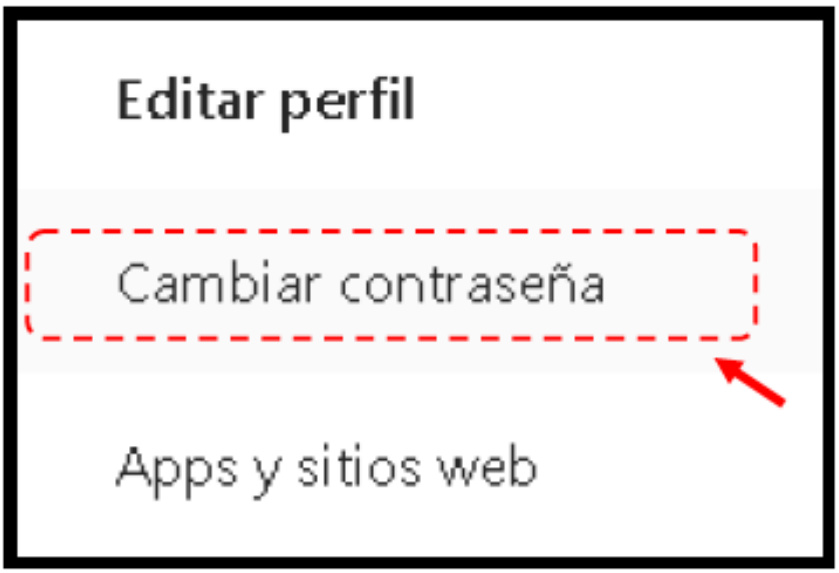
1



2



3


Editar perfil
Cambiar contraseña
Apps y sitios web

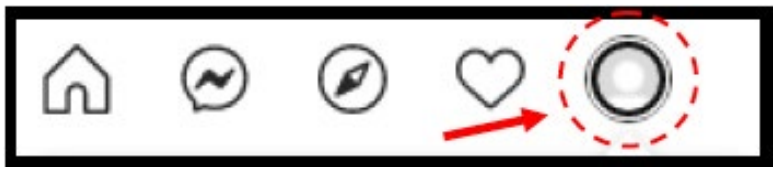
4


angyagnes7
Contraseña anterior
Contraseña nueva
Confirmar contraseña nueva
Cambiar contraseña

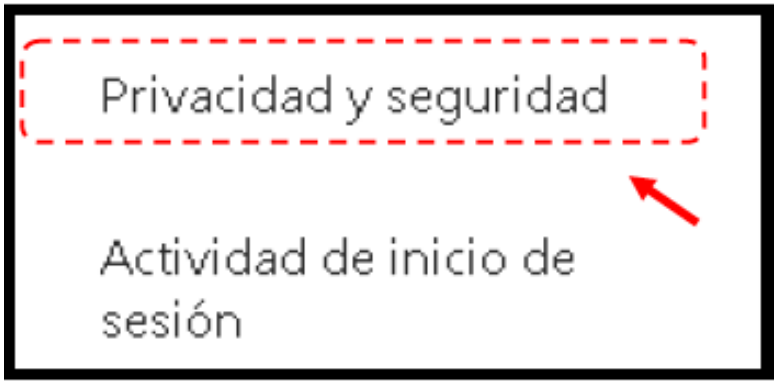
Autenticación en dos pasos para Instagram

Es un sistema para confirmar la identidad del propietario de la cuenta.

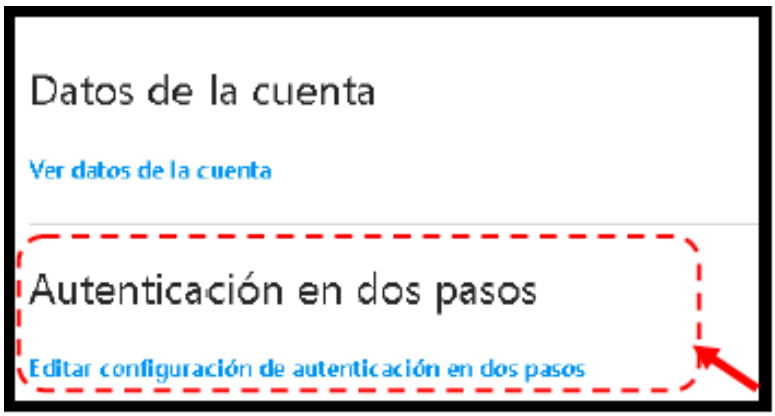
1



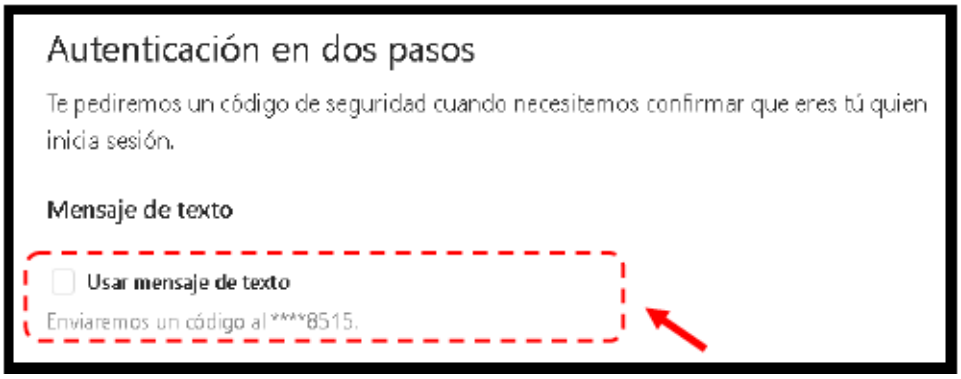
2



3



4


Autenticación en dos pasos
Te pediremos un código de seguridad cuando necesitemos confirmar que eres tú quien inicia sesión.
Mensaje de texto
Usar mensaje de texto
Enviaremos un código al ****8515.

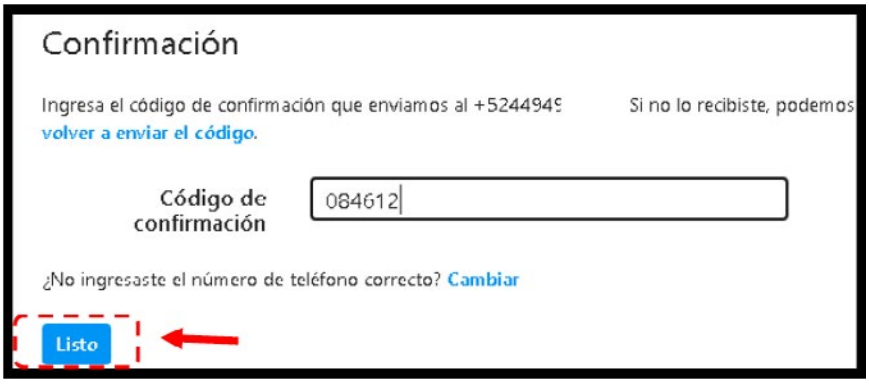
5


¿Activar?
La autenticación en dos pasos protege tu cuenta con un código adicional que debes ingresar cuando inicias sesión en un dispositivo que no reconocemos.
Activar
Ignorar

6

Verificar el número telefónico agregado en Instagram, ya que es al que será enviado el código.

7

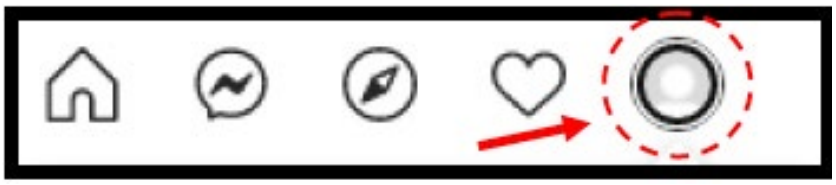


Agregar el código que fue enviado por SMS, posteriormente dar cllick en “LISTO” y el proceso a finalizado.

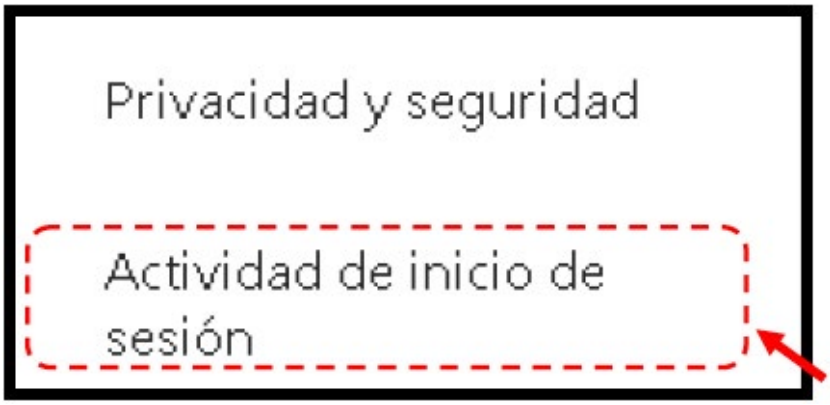
¿Quién ha iniciado sesión en tu cuenta?

Opción útil para verificar si algún tercero inició sesión con tu cuenta.

1

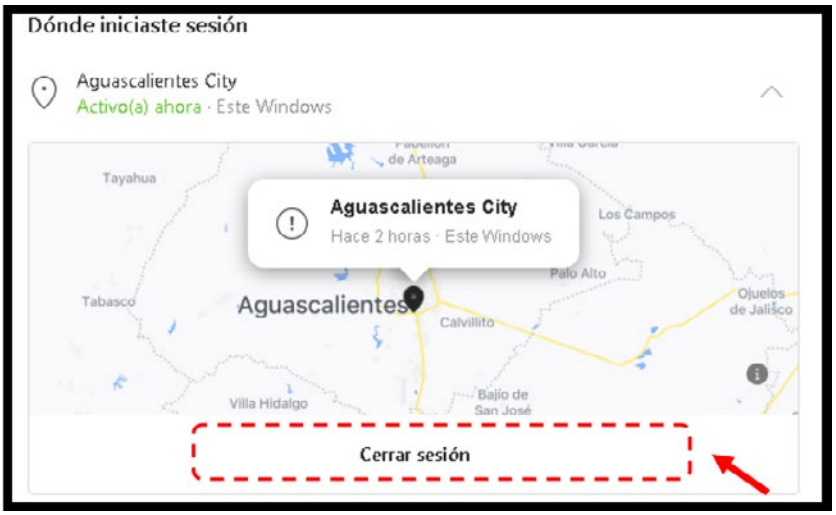


2



Verificar los inicios de sesión, en caso de que exista un dispositivo desconocido, seleccionar la opción de cerrar sesión para que dicho inicio de sesión sea finalizado.

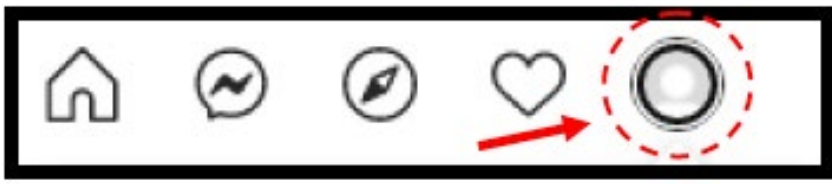
3



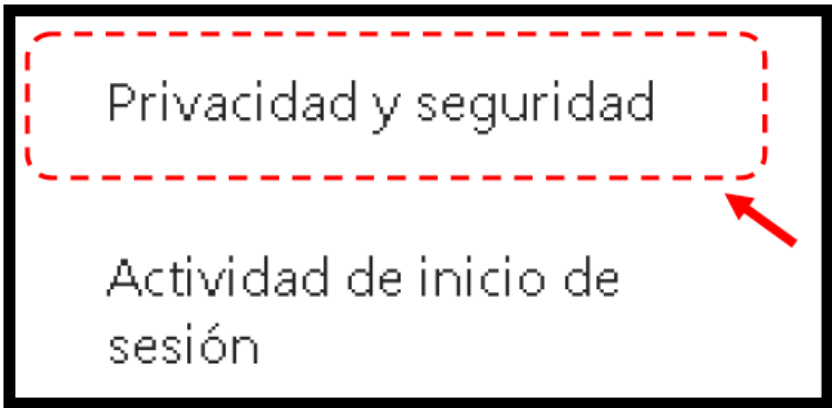
Elige si tu cuenta es pública o privada

Primer paso para gestionar la privacidad de tu cuenta de Instagram.

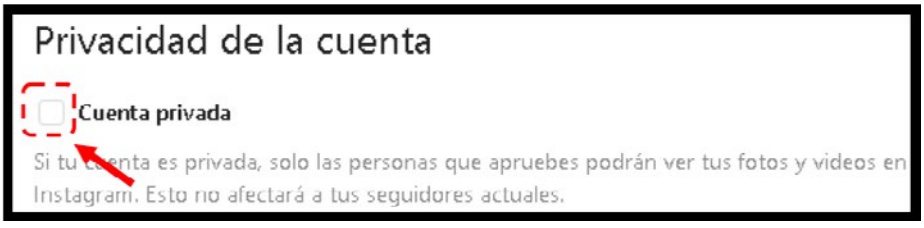
1



2



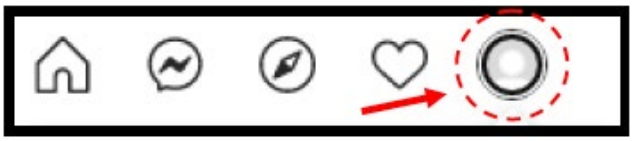
3



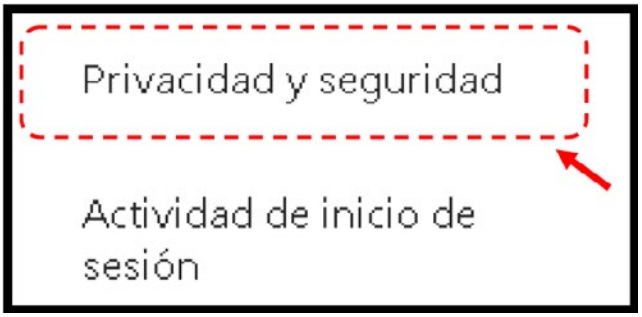
Filtro de palabras

Opción para filtrar los comentarios a través de palabras clave.

1

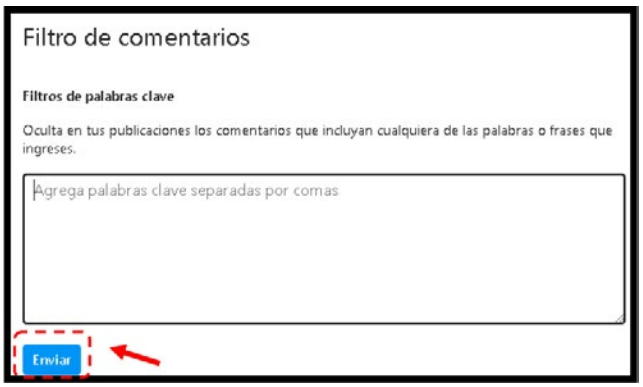


2



3

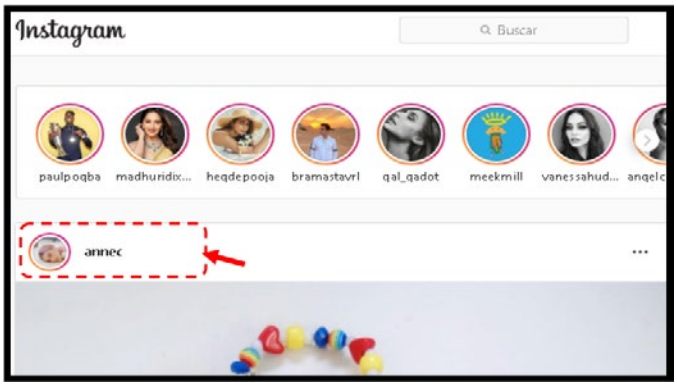
4



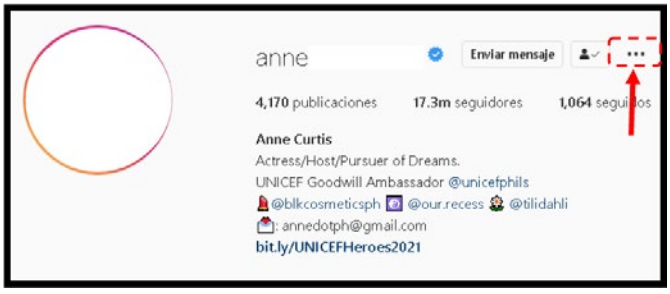
Bloquear contacto

Opción para dejar de recibir mensajes de usuarios con los que no se quiere seguir manteniendo comunicación.

1



2



3

Whatsapp

WhatsApp es una plataforma de mensajería instantánea para los teléfonos inteligentes. Es una aplicación que ha pasado a ser parte fundamental de la sociedad actual. Aproximadamente WhatsApp tiene 78 millones de usuarios en México, según ai.mx

Medidas de seguridad para evitar el robo de tu cuenta de WhatsApp

Verificacion en dos pasos

Activar un PIN de seguridad en Buzón de voz o desactivar el buzón de voz.

Evitar ingresar a link's sospechosos (ofertas en productos, empleos, noticias Fake, entre otros)

Evitar compartir información personal o códigos mediante llamadas telefónicas.

En caso de ser víctima:

Realiza la desactivación del Buzón de voz, comunicandote a tu compañía telefónica.

Desinstala tu app de WhatsApp.

Instala nuevamente tu app de WhatsApp y regístrate nuevamente (debido a que no puede estar activa la cuenta en dos dispositivos diferentes).

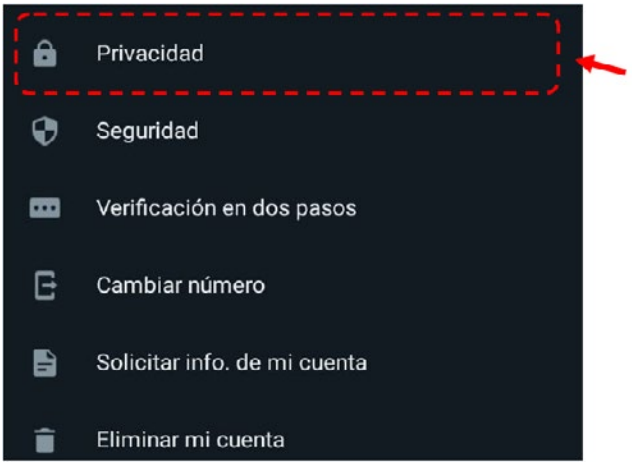
Envía un correo a WhatsApp reportando la situación: Destinatario: support@whatsapp.com, "Teléfono robado/extraviado: Por favor, desactiva mi cuenta" y adjuntando tu número de teléfono móvil con el prefijo internacional incluido (+52 lada y número).

1

Es importante elegir la opción de: Ajustes/configuración, para aplicar las siguientes medidas de seguridad

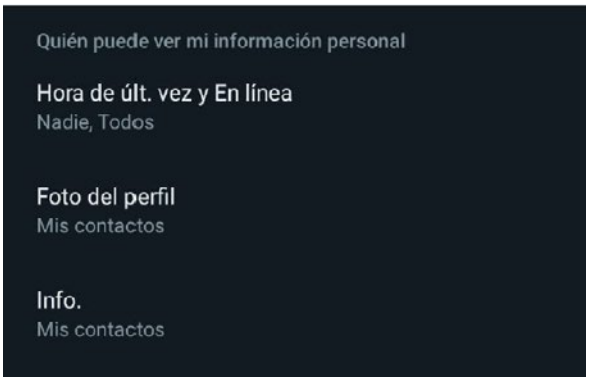
2

3



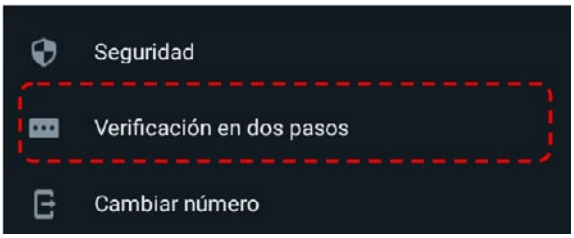
En la opción de “Privacidad” puedes seleccionar quien puede ver la información que compartes en tu cuenta, desde la hora de tu ultima conexión, fotografía de perfil, estados, entre otros.

1



Al final, se encuentra la opción de “bloqueo con huella dactilar”, una medida de seguridad aplicable para favorecer la privacidad de tu cuenta.

2



Nuevamente en el menú de cuenta (Paso 2), seleccionar “Verificación en dos pasos”, puesto que es una medida que puede evitar el robo de tu cuenta.

Twitter

Red social gratuita que se caracteriza por el envio de mensajes cortos (280 caracteres). Según DataReportal, en enero de 2022 Twitter ya contaba con más de 436 millones de usuarios activos al mes.

Conceptos básicos

- **Tweet:** término utilizado para definir un mensaje publicado en Twitter, que puede contener fotos, videos, enlaces o texto.

- **Retweet:** enviar el tweet de otra persona o usuario a tus seguidores.

- **Timeline:** La abreviación “tl” se refiere al término en inglés Timeline, y es lo que oficialmente conocemos como Cronología.

- **Follower:** seguidor

- **Hashtag:** símbolo numeral antepuesto que funciona como una etiqueta clicable a través de la cual se organizan los contenidos.

- **Trending topic:** se refiere a las tendencias, son los temas, personas o palabras más comentados en Twitter

Autenticación en dos fases

1

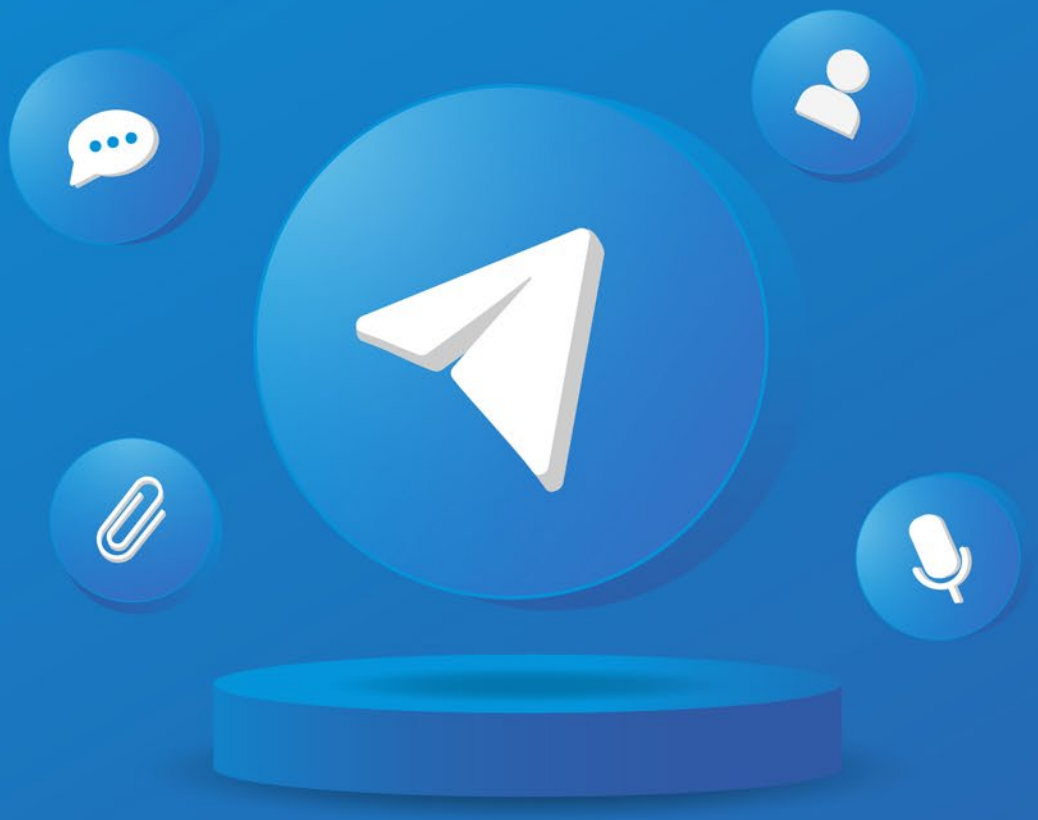
2

3

4

5

Debes seleccionar la opción que quieras utilizar



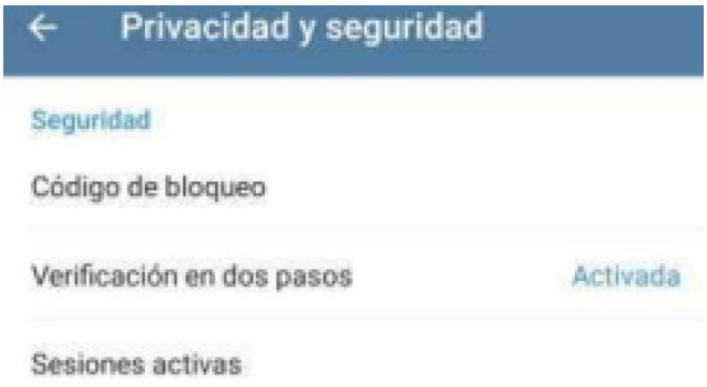
TELEGRAM

Aplicación de mensajería instantánea para dispositivos electrónicos, destaca por su sistema de seguridad y velocidad al envío de mensajes.

Verificación en dos pasos

1 Ingresa a Ajustes / configuración.

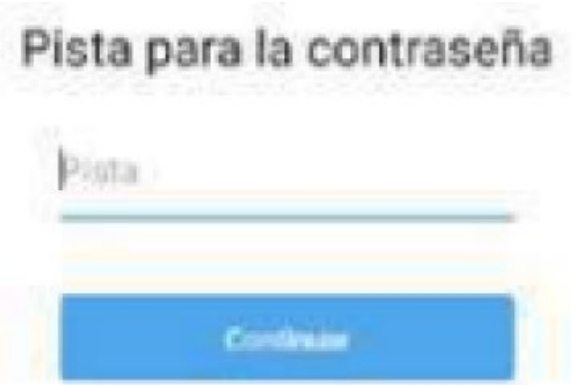
2



3

4 Selecciona Crear contraseña:

1



Puedes agregar una pista, por si llegas a olvidar la contraseña.

2

Una vez agregado el correo para recuperación, en caso de olvidar el pin, Telegram te enviara un código de 6 dígitos para la recuperación.

Videojuegos

On line

1. Descarga solo de sitios oficiales o juega en línea en sitios seguros.

2. Usa siempre mecanismos de pago oficiales.

3. Aplica medidas de protección adicionales. Verificar si alguien mas tiene acceso a tu cuenta online.

4. Desconfía de otros usuarios. De todo aquel que trate de obtener tus datos, credenciales o contraseñas.

5. Utiliza contraseñas seguras de mas de 8 caracteres, entre mayúsculas, minúsculas y números, cámbialas cada 3 meses, no las reutilices ni las compartas.

6. No olvides ajustar los parámetros de seguridad y privacidad. Para evitar que terceros tengan acceso a tu perfil, vean tu progreso o contactos.

7. Protege tu dispositivo, utiliza una red segura, mantén activos tus antivirus.

Pinterest

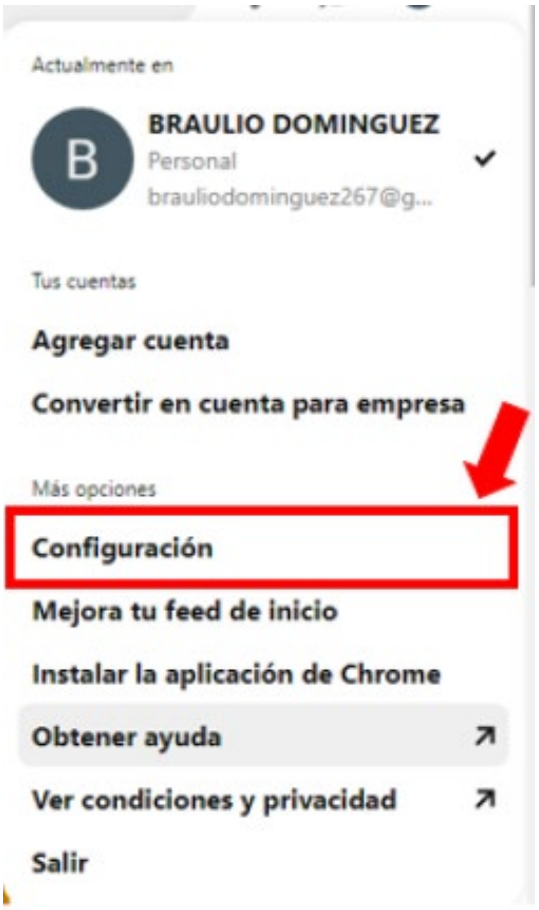
Pinterest es una red social visual, que permite a los usuarios crear y administrar, en tableros personales temáticos, colecciones de imágenes como eventos, intereses, aficiones y mucho mas. El componente social lo ponen otros pinners (usuarios) al reutilizar estas imágenes repineándolas en sus tableros.

Autenticación de dos factores

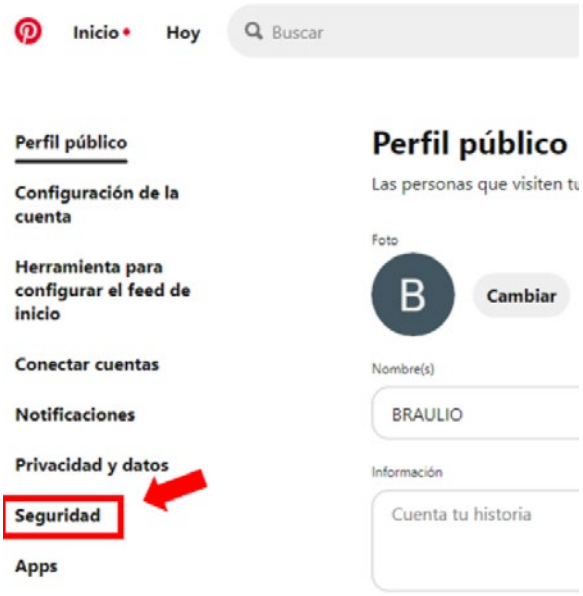
Nota: solo puedes configurar la autenticación de dos factores desde un equipo de escritorio.

1

2



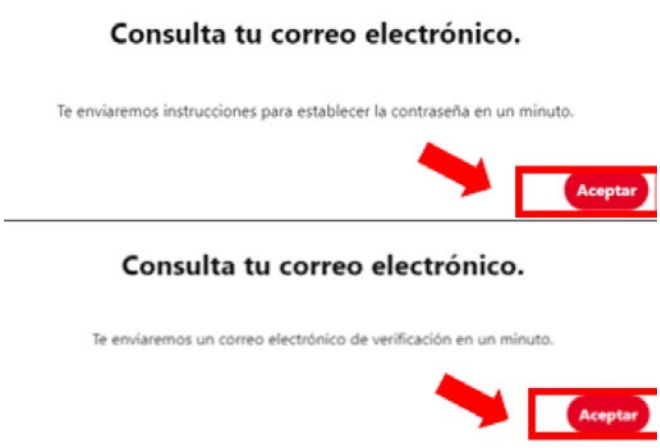
3


Inicio
Hoy
Buscar
Perfil público
Configuración de la cuenta
Herramienta para configurar el feed de inicio
Conectar cuentas
Notificaciones
Privacidad y datos
Seguridad
Apps
Perfil público
Las personas que visiten tu
Foto
B
Cambiar
Nombre(s)
BRAULIO
Información
Cuenta tu historia

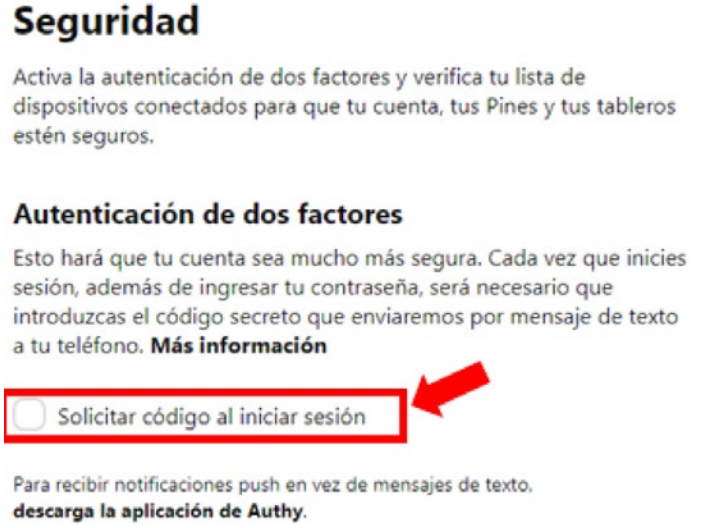
4


Seguridad
Activa la autenticación de dos factores y verifica tu lista de dispositivos conectados para que tu cuenta, tus Pines y tus tableros estén seguros.
Para activar la autenticación de dos factores, primero tienes que confirmar tu dirección de correo electrónico y establecer una contraseña.
Dispositivos conectados
Esta es la lista de los dispositivos que han iniciado sesión en tu cuenta. Anula las sesiones que no reconozcas.
Más información
Mostrar sesiones

5


Consulta tu correo electrónico.
Te enviaremos instrucciones para establecer la contraseña en un minuto.
Aceptar
Consulta tu correo electrónico.
Te enviaremos un correo electrónico de verificación en un minuto.
Aceptar

6


Seguridad
Activa la autenticación de dos factores y verifica tu lista de dispositivos conectados para que tu cuenta, tus Pines y tus tableros estén seguros.
Autenticación de dos factores
Esto hará que tu cuenta sea mucho más segura. Cada vez que inicies sesión, además de ingresar tu contraseña, será necesario que introduzcas el código secreto que enviaremos por mensaje de texto a tu teléfono. Más información
Solicitar código al iniciar sesión
Para recibir notificaciones push en vez de mensajes de texto, descarga la aplicación de Authy.

7


Contraseña
Contraseña
Para activar la seguridad de inicio de sesión, confirma tu contraseña.
¿La olvidaste?
Cancelar
Siguiente

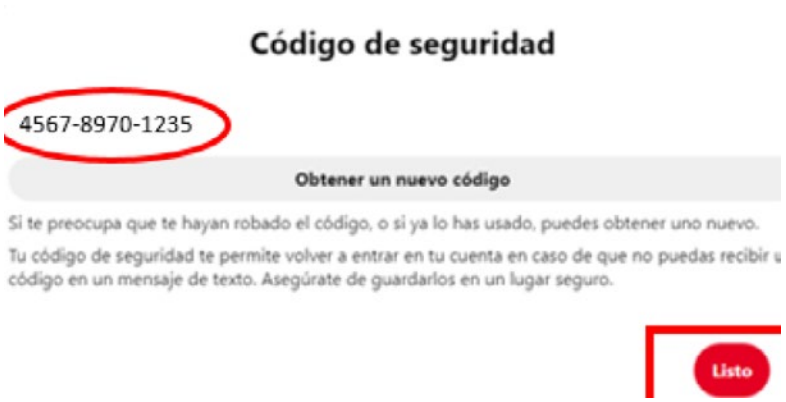
8


Número de teléfono
Código de país/región
México (+52)
Los códigos de inicio de sesión se envían aquí en un mensaje de texto.
Cancelar
Siguiente

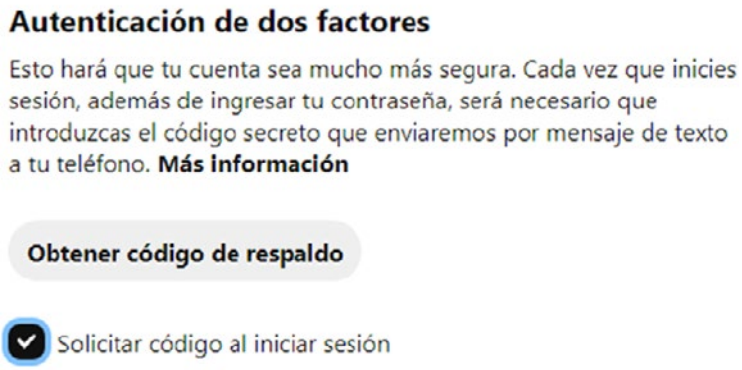
9

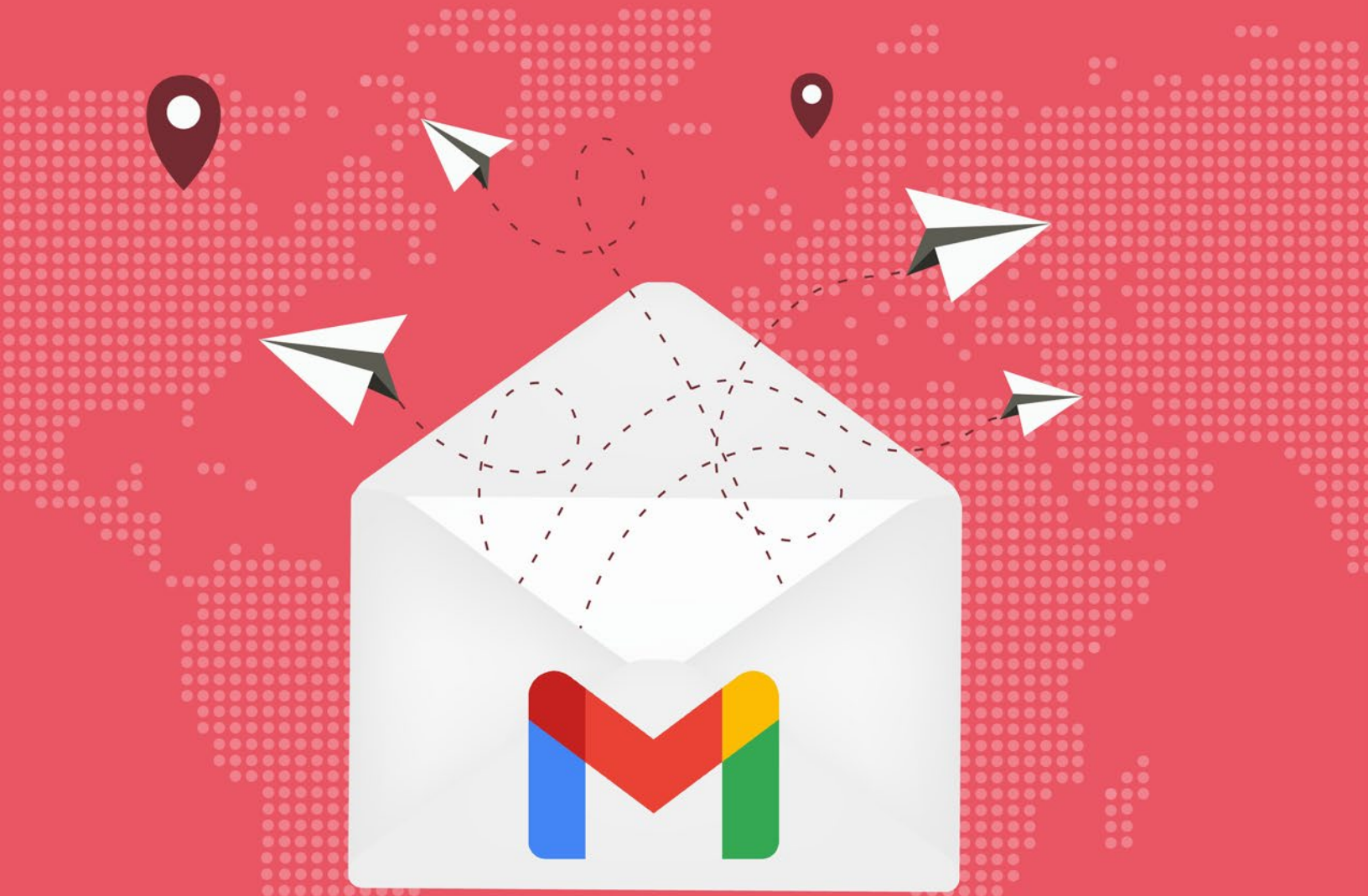

Introducir código de verificación
Ahora, introduce el código que te acabamos de enviar en un mensaje de texto a 444-444-444
Enviar código de nuevo
Cambiar número de teléfono
Cancelar
Verificar

10


Código de seguridad
4567-8970-1235
Obtener un nuevo código
Si te preocupa que te hayan robado el código, o si ya lo has usado, puedes obtener uno nuevo.
Tu código de seguridad te permite volver a entrar en tu cuenta en caso de que no puedas recibir u
código en un mensaje de texto. Asegúrate de guardarlos en un lugar seguro.
Listo

11


Autenticación de dos factores
Esto hará que tu cuenta sea mucho más segura. Cada vez que inicies sesión, además de ingresar tu contraseña, será necesario que introduzcas el código secreto que enviaremos por mensaje de texto a tu teléfono. Más información
Obtener código de respaldo
Solicitar código al iniciar sesión



Gmail

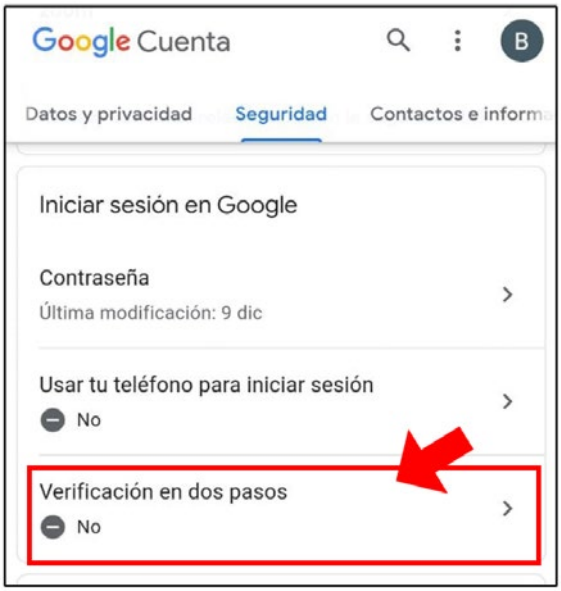
Google Gmail es un servicio de correo electrónico desarrollado por la empresa Google. Este se caracteriza por ser totalmente gratuito y multidispositivo, de forma que podemos acceder a él desde cual-quier dispositivo siempre que dispongamos de una conexión a Internet.

Verificación en dos pasos

Aplica esta medida de seguridad para reforzar tu cuenta de Gmail.

1

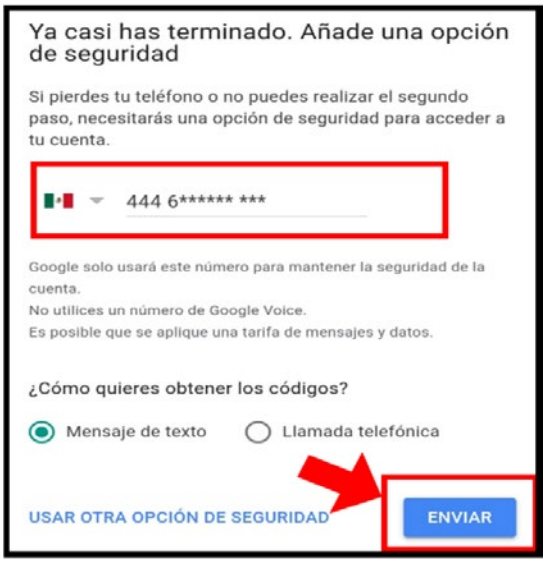
2



3


Verificación en dos pasos
Usa tu teléfono como segundo paso para iniciar sesión
Después de introducir tu contraseña, se enviarán mensajes de Google de forma segura a todos los teléfonos en los que hayas iniciado sesión. Solo tienes que tocar la notificación para revisarla e iniciar sesión.
Estos dispositivos pueden recibir mensajes
Motorola one zoom
¿No ves tu dispositivo?
Mostrar más opciones
Llave de seguridad
Se trata de un pequeño dispositivo físico que sirve para iniciar sesión.
Mensaje de texto o llamada de voz
Recibe códigos a través de un SMS o una llamada telefónica.
CONTINUAR

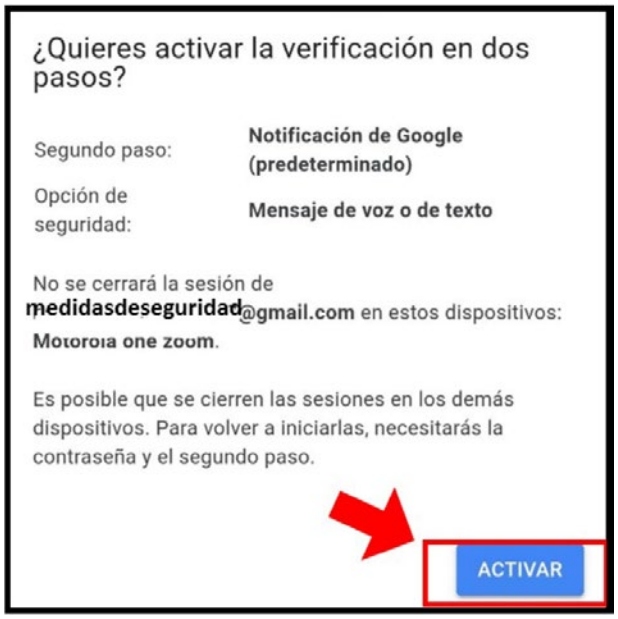
4


Ya casi has terminado. Añade una opción de seguridad
Si pierdes tu teléfono o no puedes realizar el segundo paso, necesitarás una opción de seguridad para acceder a tu cuenta.
444 6****** ***
Google solo usará este número para mantener la seguridad de la cuenta.
No utilices un número de Google Voice.
Es posible que se aplique una tarifa de mensajes y datos.
¿Cómo quieres obtener los códigos?
Mensaje de texto
Llamada telefónica
USAR OTRA OPCIÓN DE SEGURIDAD
ENVIAR

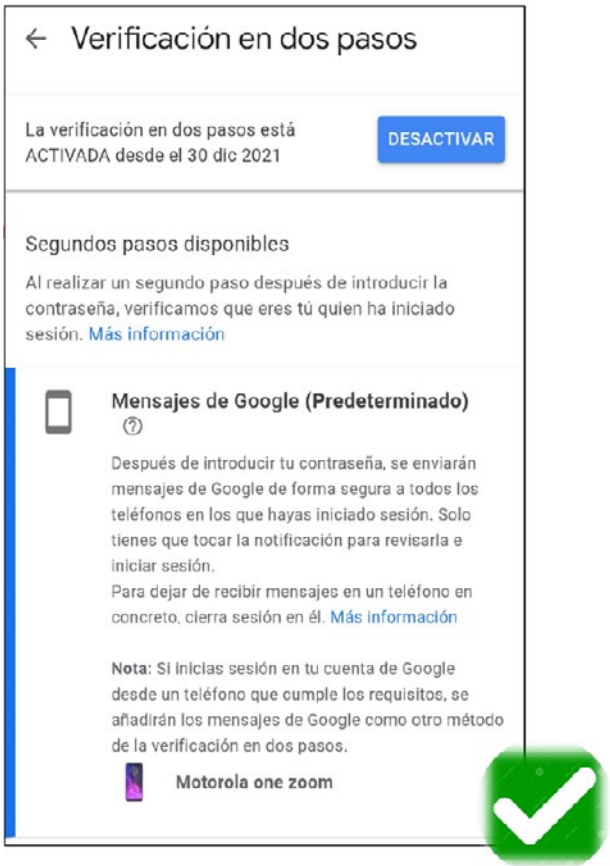
5


Confirmar que funciona
Google acaba de enviar un mensaje de texto con un código de verificación al +432 *** ***2
Introduce el código
G-457102
¿No lo has recibido? Volver a enviar
ATRÁS
SIGUIENTE

6


¿Quieres activar la verificación en dos pasos?
Segundo paso:
Notificación de Google (predeterminado)
Opción de seguridad:
Mensaje de voz o de texto
No se cerrará la sesión de medidasdeseguridad@gmail.com en estos dispositivos:
Motorola one zoom.
Es posible que se cierren las sesiones en los demás dispositivos. Para volver a iniciarlas, necesitarás la contraseña y el segundo paso.
ACTIVAR

7


Verificación en dos pasos
La verificación en dos pasos está ACTIVADA desde el 30 dic 2021
DESACTIVAR
Segundos pasos disponibles
Al realizar un segundo paso después de introducir la contraseña, verificamos que eres tú quien ha iniciado sesión. Más información
Mensajes de Google (Predeterminado)
Después de introducir tu contraseña, se enviarán mensajes de Google de forma segura a todos los teléfonos en los que hayas iniciado sesión. Solo tienes que tocar la notificación para revisarla e iniciar sesión.
Para dejar de recibir mensajes en un teléfono en concreto, cierra sesión en él. Más información
Nota: Si inicias sesión en tu cuenta de Google desde un teléfono que cumple los requisitos, se añadirán los mensajes de Google como otro método de la verificación en dos pasos.
Motorola one zoom

TikTok

Verificación en dos pasos

1

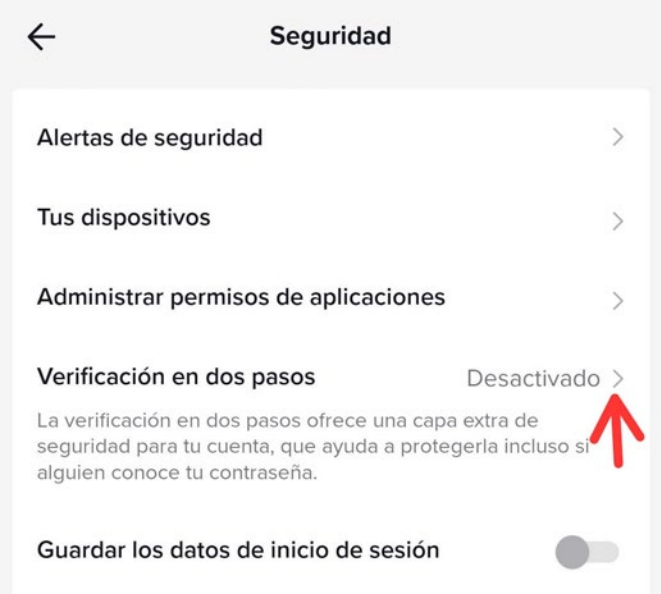
2

3

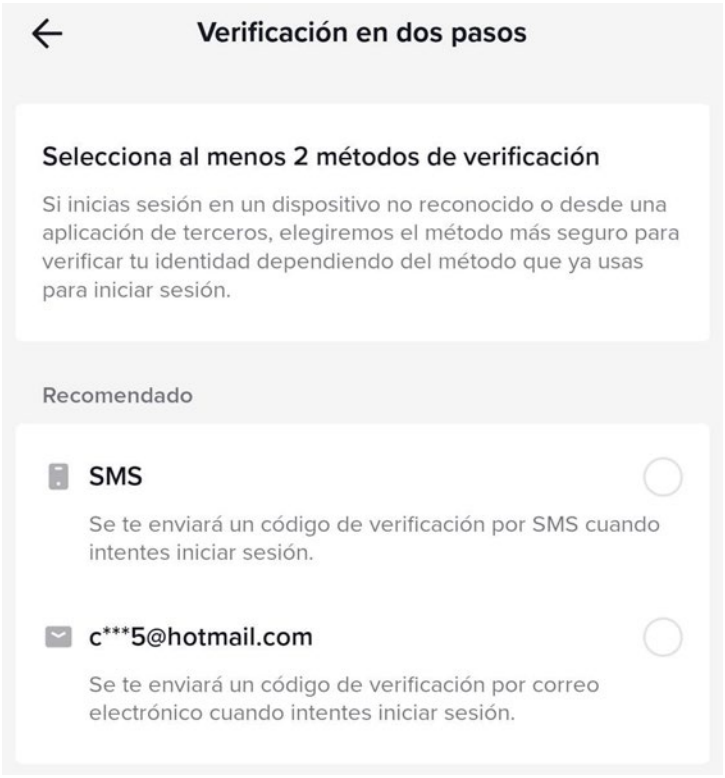
4


Ajustes y privacidad
Cuenta
Cuenta
Privacidad
Seguridad
Saldo
Compartir perfil

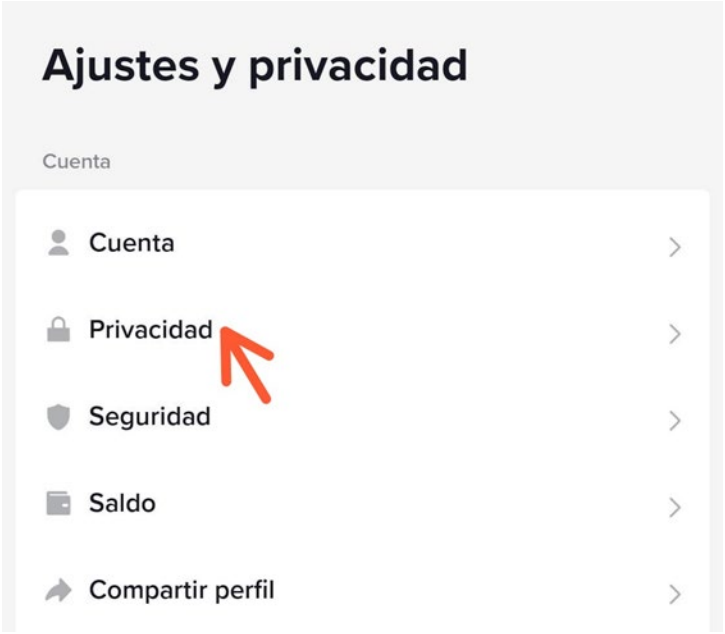
5


Seguridad
Alertas de seguridad
Tus dispositivos
Administrar permisos de aplicaciones
Verificación en dos pasos
Desactivado
La verificación en dos pasos ofrece una capa extra de seguridad para tu cuenta, que ayuda a protegerla incluso si alguien conoce tu contraseña.
Guardar los datos de inicio de sesión

6

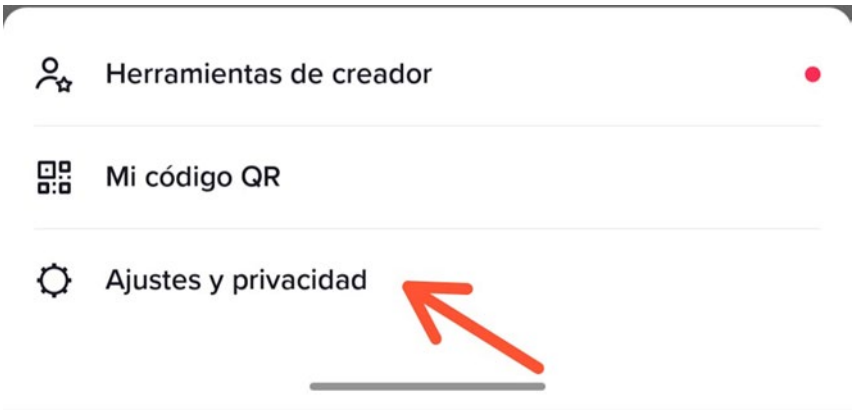

Verificación en dos pasos
Selecciona al menos 2 métodos de verificación
Si inicias sesión en un dispositivo no reconocido o desde una aplicación de terceros, elegiremos el método más seguro para verificar tu identidad dependiendo del método que ya usas para iniciar sesión.
Recomendado
SMS
Se te enviará un código de verificación por SMS cuando intentes iniciar sesión.
c***5@hotmail.com
Se te enviará un código de verificación por correo electrónico cuando intentes iniciar sesión.

7


Ajustes y privacidad
Cuenta
Cuenta
Privacidad
Seguridad
Saldo
Compartir perfil

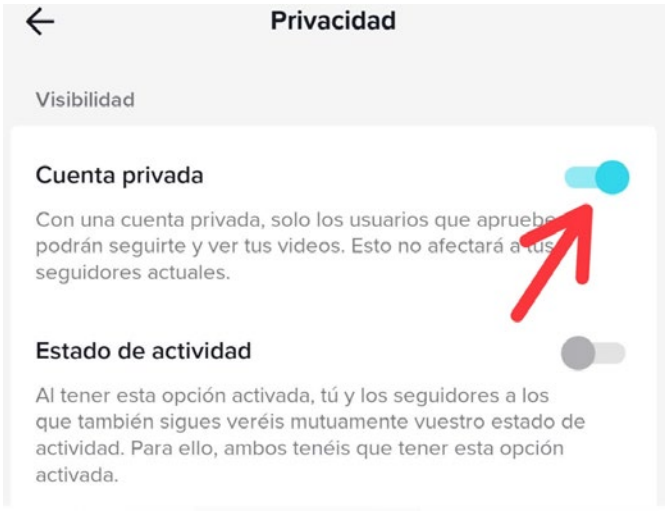
Privatiza tu cuenta de TikTok

1



2

3



Medidas de seguridad que debes tomar en las aplicaciones de tu móvil

- **No compartas tu contraseña.**
- **Configura tu privacidad en tus redes sociales y revísala con frecuencia.**
- **Verifica los accesos que tienen las aplicaciones en tu teléfono.**
- **Limita la visibilidad de tu información.**
- **Crea una contraseña compleja y difícil de adivinar.**
- **Utiliza el "filtro estricto" para recibir mensajes de sus contactos o amigos de Facebook.**
- **Oculta tu correo electrónico en tus cuentas.**
- **Cambia tu contraseña constantemente.**
- **Evita conectarte a una red Wifi gratuita.**
- **Evita poner tu foto en tu perfil.**
- **Evita poner tus datos personales en el perfil de tus redes sociales.**
- **No aceptes solicitud de amistad de personas desconocidas.**
- **No proporciones información personal , ni datos bancarios a personas desconocidas.**
- **Elige que tus contactos sean conocidos y de confianza.**
- **Elige bien quien pude ver tus publicaciones.**

- ***Lic. Crim: Alejandra Patricia Chávez Arias:*** “Por la libertad, los derechos digitales y seguridad en el ciberespacio”

- ***Lic. Cynthia Karina Cruz Franco:*** “No deseo que las mujeres tengan más poder que los hombres, sino que tengan más poder sobre sí mismas” Mary shelley

- ***Lic. Arely Betsabe Gaytán Rosales:*** “La Sororidad debe ser un hecho, no simplemente una palabra”

- ***Lic. Lizeth Ramona Moreno Marmolejo:*** “El acto más valiente sigue siendo pensar por ti misma. En voz alta. La violencia a través de los medios digitales también es un delito. ¡Denuncia! ¡Somos libres!

- ***Lic. Janeth Salazar Arias:*** “La vida es un reto; vívela, siente, ama, ríe, llora, juega, gana, pierde, tropieza, pero siempre levántate y sigue.”

- ***Lic. Miriam Alejandra Duron Pérez:*** “Cuando una mujer decide cambiar, todo a su alrededor también cambia.” Eufrosina cruz.

- ***Lic. Nora Alejandra Leyva Noriega:*** “La paciencia es un árbol de raíz amarga pero de frutos muy dulces.” Proverbio Persa

- ***Lic. Yolanda Muñoz Iñiguez:*** “Defiende tu derecho a pensar, porque incluso pensar de manera errónea es mejor que no pensar” Hipatia