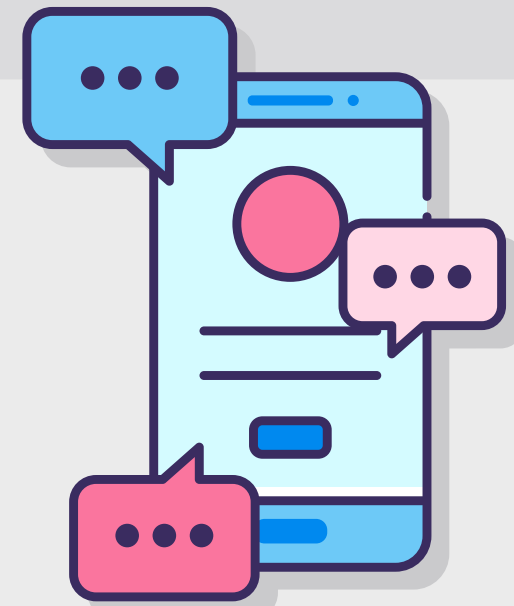


Seguridad y confianza en mensajería instantánea

Los programas de mensajería instantánea permiten enviar y recibir mensajes, imágenes, voz o video con tus contactos de manera simultánea por medio de un servicio de internet o de datos.

¿Cómo funcionan?

Estos programas permiten comunicación sincrónica o asincrónica con tus contactos a través de **un servidor que recibe, almacena y envía los mensajes**. Hay distintos programas que sirven para conversar en línea pero todos funcionan un poco diferente. **Algunos son más seguros que otros.**



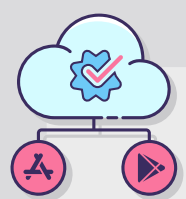
Los riesgos de comunicarse por mensajería

Si no tienes cuidado las conversaciones que tienes **pueden ser leídas por alguien más**. Si el desarrollador de la aplicación no tiene las medidas necesarias de protección, tus mensajes también pueden ser leídos por alguien que esté monitoreando tu conexión a internet o incluso el mismo proveedor puede tener acceso a tus mensajes. Si los proteges de la manera adecuada ninguno de estos podrá saber qué dices. **De esta forma proteges tu privacidad**

Riesgos de la mensajería instantánea sin cuidados:

- **Vigilancia.**
- **Robo** de dispositivos y datos.
- **Acoso y extorsión.**
- **Falsificación de identidad.**
- **Espionaje.**

Medidas de seguridad



Utiliza las aplicaciones de mensajería instantánea de Google Play o de App Store. **Asegúrate que son las aplicaciones oficiales.**

Aquí veremos:



Signal

y



WhatsApp

[<https://signal.org>]

[<https://www.whatsapp.com>]



Cifrado. Prefiere las aplicaciones de mensajería instantánea que **cifran***"de extremo a extremo". De esta manera, solo tú y tu contacto podrán saber el contenido de la conversación. **Los programas de mensajería más populares que cifran de extremo a extremo son: Signal y Whatsapp.**

Telegram tiene cifrado de extremo a extremo solo cuando se activa el chat secreto

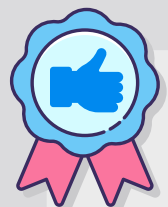
*El cifrado es un método que codifica y distorsiona los mensajes o datos para que solo las personas que comparten una clave puedan saber el contenido del mensaje.

Generación y gestión segura de contraseñas

Medidas de seguridad



Contraseñas. Algunas aplicaciones tienen una contraseña propia. Asegúrate que tu dispositivo se bloquee y que tenga una buena contraseña. También agrega una contraseña a tu aplicación de mensajería. En este caso, solo Signal tiene contraseña de bloqueo de aplicación, Whatsapp bloquea la aplicación por medio de tu huella o Face ID.



Reputación. Revisa las calificaciones y comentarios que hacen otros usuarios de la aplicación de mensajería que quieres probar. Busca la cantidad de descargas que tiene y la fecha de su última actualización. Así te puedes dar una mejor idea sobre qué tal funciona.

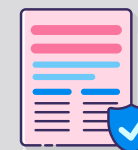


Verificación. Algunas aplicaciones de mensajería permiten verificar a tus contactos. De esta forma puedes estar seguro que te estás comunicando con quien te quieres comunicar y no es alguien más haciéndose pasar por esta persona. Tanto Signal como Whatsapp permiten verificar a tus contactos.



Borrado automático de mensajes. Otra medida que puede evitar que alguien que tenga acceso a tu teléfono no vea tus conversaciones es que los mensajes se borren automáticamente después de un periodo de tiempo.

Hasta ahora solo Signal tiene esta opción.



Permisos. Revisa los permisos que pide la aplicación para acceder a tus datos y partes del dispositivo. Los permisos los puedes revisar en el repositorio oficial de la aplicación antes de que la instales pero también en las configuraciones del sistema operativo. En Android: Configuración > Apps y notificaciones > Información de la aplicación > Permisos.

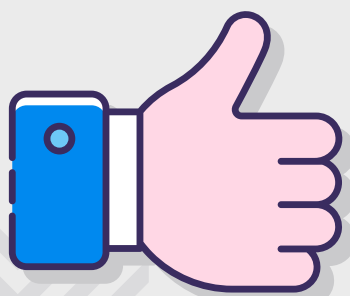
En iOS: Configuración > Privacidad > Aplicaciones que tienen permiso. También puedes ver información sobre los permisos de varias aplicaciones en:

<https://reports.exodus-privacy.eu.org>



Actualizaciones. Recuerda mantener actualizados tus programas, incluyendo las aplicaciones de mensajería que uses.

Recomendaciones generales



La seguridad digital no solo depende del programa que usas sino también de ti y de las personas con quienes te comunicas. Procura mantener un entorno de confianza con tus contactos, usando aplicaciones seguras y teniendo buenas prácticas para cuidar tu información y la de los demás.

Las medidas de seguridad digital dependen del tipo de información, dónde está guardada y cómo la envías. Para tomar mejores medidas es necesario que tengas en cuenta tu entorno, lo que quieres proteger y de quién. Con base en esto, elige la opción que más te sea útil y que no sacrifique tu seguridad y privacidad.

Distingue los distintos tipos de conexiones que usas al comunicarte y procura usar la red en la que tengas más confianza.

Otras alternativas

Existen distintas alternativas para comunicarte además de las mencionadas anteriormente.

Quizás vale la pena que las pruebes. Recuerda revisar cómo funcionan en el sitio oficial y otras fuentes antes de confiarles información importante.



<https://silence.im>



<https://delta.chat>



TOX <https://tox.chat>



<https://about.riot.im>



BRIAR <https://briarproject.org>