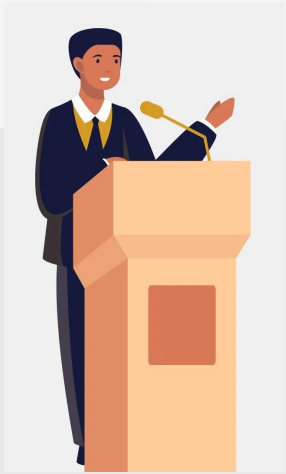
SIGNAL

Alejandro Anaya
Gustavo Jiménez
Ángel Santander

TABLA DE CONTENIDOS



01

Introducción

Signal como una aplicación de mensajería

Signal

Whisper Systems

Dos servicios de código abierto:
Text Secure
Red fone

Fundada por

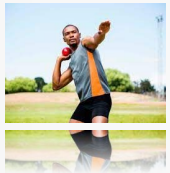
- Investigador de seguridad Moxie Marlinspike
- Desarrollador Stuart Anderson

Proyecto de código abierto

Open Whisper Systems

Primer actividad del proyecto

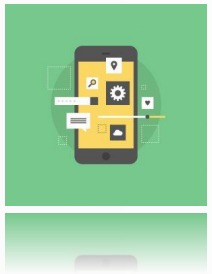
Desarrollo del protocolo Signal, con cifrado extremo a extremo



29 de julio del 2014

Se lanza Signal inicialmente en iOS

En 2015 en Android

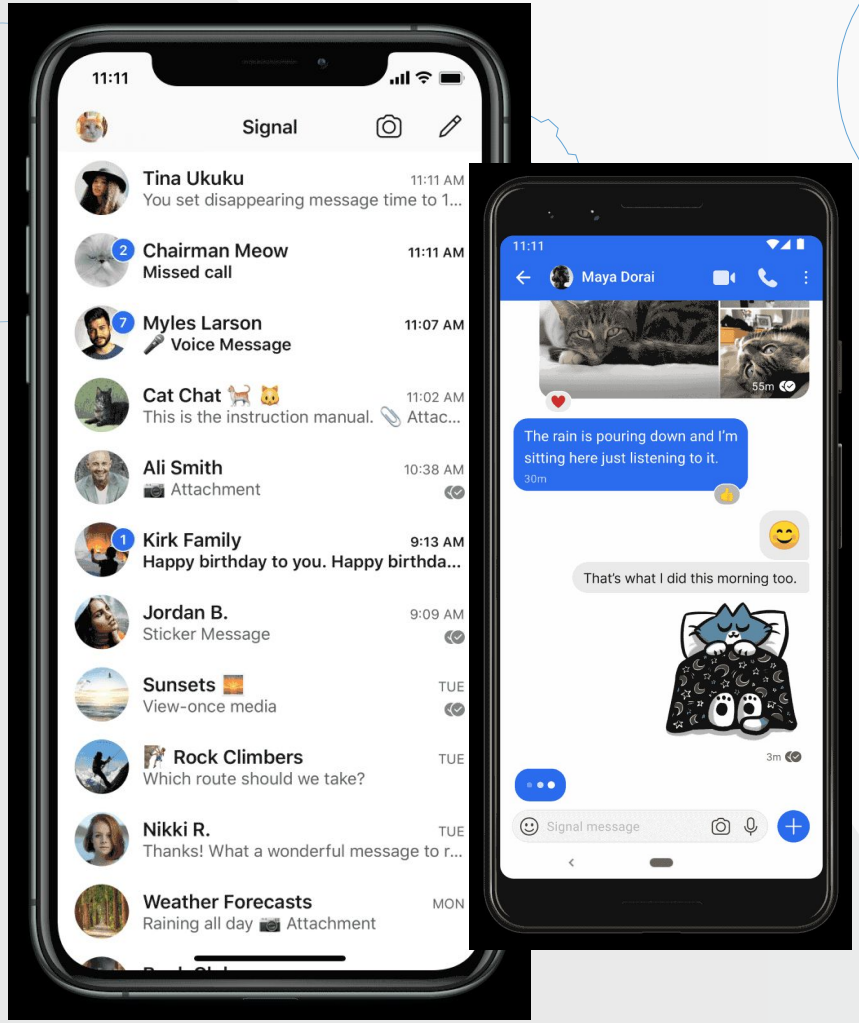


Aplicación

Diseñada para comunicación

Características

¿Para qué se utiliza?



— Descripción de Signal

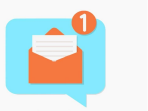
Signal es una aplicación unificada gratuita, sencilla, de código abierto, que proporciona llamadas de voz y mensajería de textos privados (Greenberg, 2015).

Principales características

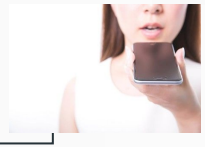
Mensajes

Envío de contactos y ubicación

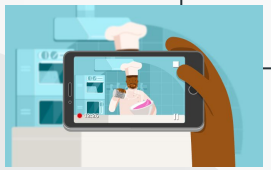
Creación de grupos



Notificaciones



Enviar fotos, videos, GIFs, archivos

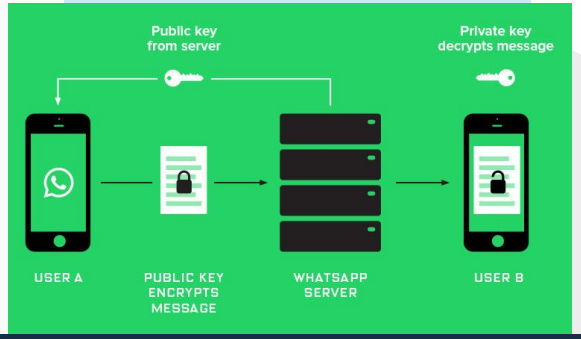


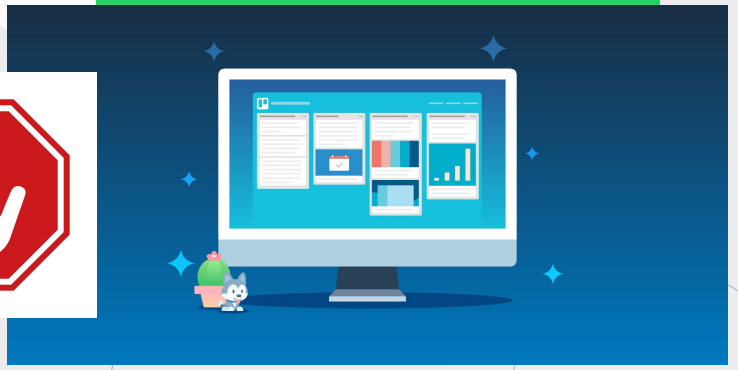
Videollamadas, llamadas y notas de voz

Personalización

Tecnología

Cifrado extremo a extremo (AES-GCM-SIV)
Protocolo de cifrado Signal
Aplicación de escritorio
Desbloqueo nativo de la plataforma
Bloqueo de capturas de pantalla en la app
Licencia GPL y AGPL (Open Source)
Para cada plataforma se requiere: iOS igual o posterior a 11.1,
Android igual o posterior a 4.4,
Windows 64 bits: 7, 8, 8.1 y 10,
MacOS 10.12 y superiores,
O distribuciones de 64 bits de Linux





AGPL Free Software

GPL Free Software

03

Modelo de negocio

Logo de Open Whisper Systems

Al contrario de otros competidores como Facebook y Telegram, Signal no es un negocio y por lo que realmente no tiene un modelo de negocio en el sentido tradicional. Open Whisper Systems es un proyecto colectivo compuesto por voluntarios y un número creciente de contribuyentes, que a veces reciben donativos y subvenciones.

Donaciones

Menos del 1 por ciento de los usuarios de Signal donan a Open Whisper Systems
En 2018, recibió $ 600,000 en donaciones, pero gastó $ 4 millones en personal e infraestructura.
También en 2018 el cofundador de WhatsApp, Brian Actor, le otorgó a Signal un préstamo sin interés de 105 millones de dólares.

Usuarios

Fecha	Usuario
• Diciembre del 2010	• 0.5 Millones
• Julio del 2020	• 3.5 Millones
• December 2020	• 20 Millones
• January 2021	• 40 Millones

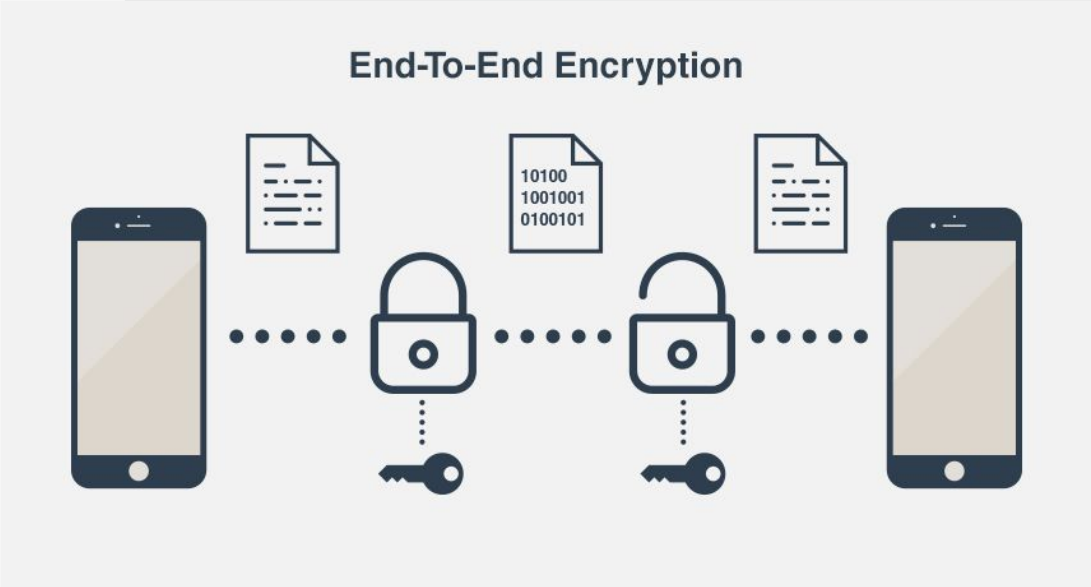
Descargas

Fecha	Usuario
Mayo del 2020	11 Millones
Enero del 2021	41 Millones
Mayo del 2021	105 Millones

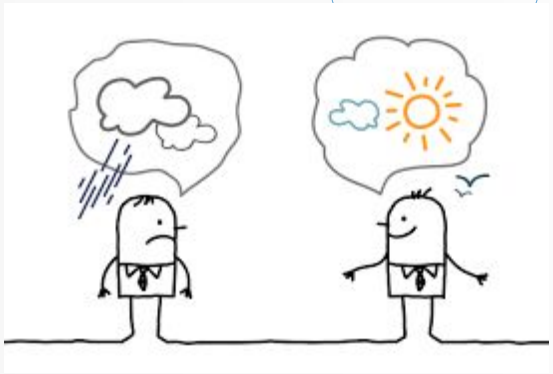
04

Seguridad

Utiliza un criptosistema de clave pública dónde hay una pública y otra privada, la llave pública de un usuario se intercambia con todos los demás usuarios que van a enviar mensajes con este además cifra los mensajes mientras que la privada es utilizada para descifrar los mensajes cifrados con la llave pública y se almacena de manera local.



En Signal la llave privada se almacena de manera local en el dispositivo utilizando la base de datos SQlite con la extensión SQLCipher, la llave privada es cifrada utilizando el algoritmo AES-256 y esta permanece en el dispositivo del usuario sin ser enviada.



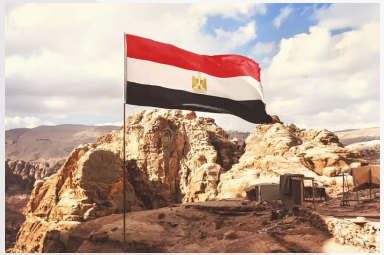
05

Popularidad, implicaciones y problemáticas políticas

El 7 de enero del 2021 Elon Musk recomienda Signal para sustitución de Whatsapp, alzando su popularidad entre los usuarios de los diferentes sistemas operativos.

Países donde Signal más usado

BLOQUEOS



Egipto bloqueo Signal en 2016, como respuesta por parte del de la plataforma se agregó un frente de dominio a su servicio, permitiendo a los usuarios eludir la censura.

Irán bloqueo signal en 2018, para enero del 2021 elimina la aplicación de las tiendas de aplicaciones.

China bloquea Signal en marzo de 2021.

"La misma tecnología que mantiene una conversación privada entre usted y un miembro de la familia, también brinda un refugio seguro a un terrorista en Siria y a la persona en los Estados Unidos que está tratando de reclutar para cometer un acto de asesinato masivo".

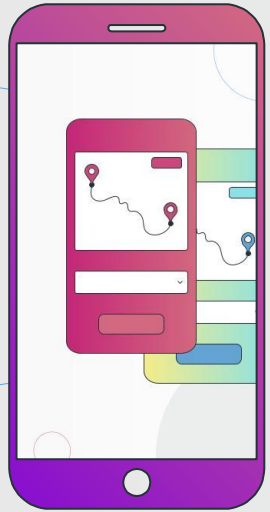
CNN

Autoridades de la India arrestan en 2016 a miembros de una célula terrorista presuntamente afiliada a ISIS que se comunicaba a través de Signal y Telegram

Milicias de derecha y nacionalistas blancos utilizaron Signal para organizar sus acciones, incluida la manifestación Unite the Right II en 2018.

06

Conclusiones



PROS

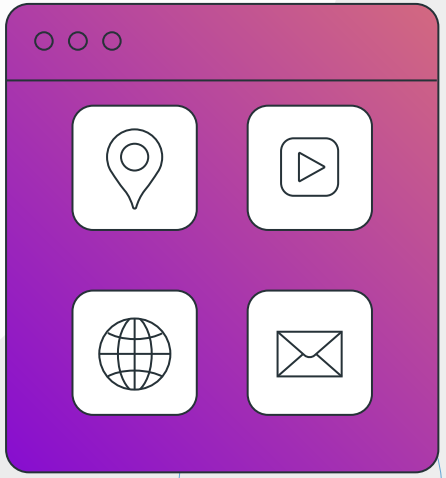
- Máxima seguridad en chats.
- Disponible en diversos S.O.
- Presentación y uso amigable.
- Gratuita

CONTRAS

- Por su privacidad, puede tener un mal uso.
- Se mantiene a base de donaciones.
- Falta de popularidad.
- Mucha competencia.

Posibles mejoras

- Registro de una cuenta sin necesidad de contar con un número de teléfono
- Creación de canales
- Bots
- Canales de voz
- Capacidad para compartir pantalla
- Aplicación de escritorio nativa para un mayor performance
- Minijuegos dentro de la aplicación
- Permitir utilizar la misma cuenta Signal en distintos dispositivos móviles
- No mostrar la leyenda de que un mensaje fue eliminado
- Desvinculación de referencia de los mensajes eliminados
- Sincronización entre las bases de datos locales de los dispositivos



Referencias

1. Lumb, D. (2018, 1 noviembre). The story of Signal. Recuperado 22 de octubre de 2021, de https://increment.com/security/story-of-signal/
2. Greenberg, A. (2015, 3 noviembre). Signal, the Snowden-Approved Crypto App, Comes to Android. Recuperado 22 de octubre de 2021, de https://www.wired.com/2015/11/signals-snowden-approved-phone-crypto-app-comes-to-android/
3. El comercio. (2021, 11 enero). ¿Qué es Signal, cuáles son sus características y qué ventajas ofrece a los usuarios? Recuperado 22 de octubre de 2021, de https://elcomercio.pe/respuestas/whatsapp-que-es-signal-y-cuales-son-sus-caracteristicas-y-ventajas-mensajeria-instantanea-revlti-noticia/
4. GNU. (s. f.). The GNU General Public License v3.0 - GNU Project - Free Software Foundation. Recuperado 22 de octubre de 2021, de https://www.gnu.org/licenses/gpl-3.0.html
5. GNU. (2007, 19 noviembre). GNU Affero General Public License - GNU Project - Free Software Foundation. Recuperado 22 de octubre de 2021, de https://www.gnu.org/licenses/agpl-3.0.en.html
6. Signal Support. (s. f.). Security check. Recuperado 22 de octubre de 2021, de https://support.signal.org/hc/es/articles/360007211952-Soluci%C3%B3n-de-problemas-con-las-instalaciones-o-actualizaciones
7. Curry, D. (2021, 7 junio). Signal Revenue & Usage Statistics (2021). Recuperado 22 de octubre de 2021, de https://www.businessofapps.com/data/signal-statistics/
8. Signal Messenger. (2020, 2 junio). Logo of Signal [Ilustración]. Recuperado de https://upload.wikimedia.org/wikipedia/commons/6/6a/Signal-logo.png
9. Signal. (s. f.). Signal para dispositivos móviles [Ilustración]. Recuperado de https://signal.org/assets/screenshots/download-mobile-bdc14a52a345c02611f4a8ac2a2796dfd4f5f2d9cf9abbf2494bd3e244d63035.png