Signal

GUÍA DE PRIVACIDAD

Signal

Los principios, sin tecnicismos

Qué es, cómo protege tus mensajes y por qué es tan fiable.

01

Qué es Signal

Signal es una aplicación de mensajería y llamadas pensada para que solo tú y la persona con quien hablas podáis leer lo que os decís. La mantiene una fundación sin ánimo de lucro, sin publicidad, y sus protocolos de cifrado se han convertido en la referencia del sector.

CIFRADO DE EXTREMO A EXTREMO

Los mensajes y las llamadas se cifran en tu móvil y solo se abren en el de tu contacto. Ni Signal puede leerlos.

SIN PUBLICIDAD

La financian donaciones y suscripciones voluntarias, no la venta de datos ni los anuncios.

CÓDIGO ABIERTO

Cualquiera puede leer cómo funciona, revisarlo y proponer mejoras.

02

Cuatro ideas previas

Si ya sabes cómo funciona el cifrado, salta directamente a la sección 4.

1. **Las claves.** Tienes dos números enlazados. La clave pública es como el número de tu buzón: puedes dárselo a cualquiera. La clave privada es la llave que lo abre, y no sale nunca de tu móvil.
2. **El cifrado de extremo a extremo.** El mensaje se convierte en datos ilegibles al salir de tu móvil y solo se vuelve legible al llegar al del destinatario. Los servidores por los que pasa solo ven ruido.
3. **Los metadatos.** Son los datos sobre la conversación, no su contenido: quién habla con quién, cuándo y desde dónde. A veces cuentan tanto como el propio mensaje.
4. **La verificación.** Para estar seguro de que la clave que recibes es realmente la de tu contacto, ambos podéis comparar un número que depende de las dos claves. Si coincide, nadie se ha puesto en medio.

03

El problema: casi nadie sabe por dónde pasan sus mensajes

Un mensaje recorre varios ordenadores antes de llegar. Si el servicio solo cifra la conexión con su servidor, la empresa puede leer todo lo que pasa por allí, guardarlo o entregarlo si se lo piden. Y aunque el contenido esté protegido, la empresa sigue sabiendo con quién hablas y cuándo: es como si el sobre estuviera cerrado, pero el cartero apuntara en un cuaderno cada remitente y cada destinatario.

> **Por qué importa.** Quien conoce tus contactos y tus horarios puede deducir mucho de ti sin abrir un solo mensaje. Una buena mensajería tiene que proteger el contenido y reducir también lo que sabe de las personas.

04

Los tres principios de privacidad

Signal protege tres cosas a la vez, cada una con su propia técnica.

CONTENIDO

Solo vosotros lo leéis

Cifrado de extremo a extremo.

HISTORIA

Una llave nueva por mensaje

El doble trinquete.

METADATOS

El servidor sabe lo mínimo

Remitente sellado y contactos privados.

Contenido: solo vosotros lo leéis

Antes de escribir, tu móvil y el de tu contacto se ponen de acuerdo en una llave secreta usando sus claves públicas, aunque nunca se hayan visto y aunque alguien escuche todo lo que se dicen. Con esa llave, el mensaje se cifra en tu móvil. El servidor recibe un paquete

cerrado y lo guarda hasta que el destinatario se conecta. Es como dos personas que, hablando en voz alta en una plaza, consiguen acordar un código que nadie más puede deducir.

Historia: una llave nueva en cada mensaje

La llave no es siempre la misma: cambia con cada mensaje y cada vez que la conversación cambia de turno. Se llama el doble trinquete porque, como un trinquete mecánico, solo gira en un sentido: de la llave de hoy no se puede deducir la de ayer. Si alguien te robara el móvil hoy, no podría leer los mensajes antiguos, y si copiara tus llaves, la conversación se cura sola en cuanto os escribís de nuevo.

Metadatos: el servidor sabe lo mínimo

Signal reduce lo que su propio servidor puede ver. Con el remitente sellado, el servidor sabe a quién va el mensaje, pero no de quién viene. Para encontrar a tus contactos usa un procesador protegido por hardware que busca los números sin que nadie, ni el propio Signal, vea tu agenda. En los grupos, los nombres y los miembros se guardan cifrados. Y puedes crear un nombre de usuario para no dar tu número de teléfono a desconocidos.

> Los tres mecanismos funcionan juntos: el contenido va protegido, las llaves no duran y el servidor ve lo mínimo necesario para entregar.

05

Un mensaje, paso a paso

1. Tu aplicación pide al servidor las claves públicas de tu contacto, que este dejó preparadas aunque esté desconectado.
2. Con ellas, tu móvil calcula una llave secreta compartida, reforzada con un secreto poscuántico.
3. Cifra el mensaje con una llave de un solo uso y la borra después.
4. Lo envía al servidor dentro de un sobre sellado: se ve el destinatario, no el remitente.
5. El servidor lo guarda hasta que tu contacto se conecta. Nunca puede abrirlo.
6. El móvil de tu contacto lo descifra y la conversación avanza a una llave nueva.

06

Cómo sacarle partido

UN PIN LARGO

Protege tu cuenta si alguien intenta registrar tu número en otro teléfono. Activa también el bloqueo de registro.

UN NOMBRE DE USUARIO

Te permite chatear sin dar tu número de teléfono y decidir quién puede encontrarte con él.

VERIFICAR CONTACTOS

Compara el número de seguridad o usa la verificación automática para saber que hablas con quien crees.

MENSAJES TEMPORALES

Se borran solos pasado el tiempo que elijas, en las conversaciones más delicadas.

Signal está preparado para el futuro: ya combina cifrado clásico con cifrado resistente a ordenadores cuánticos, de modo que lo que envías hoy siga protegido mañana. Ningún sistema puede proteger un móvil que ya esté en manos de otra persona o infectado, así que mantén el sistema actualizado y bloquea la pantalla.

REFERENCIA

Glosario rápido

TÉRMINO	EN UNA FRASE
Cifrado de extremo a extremo	Solo los dos extremos de la conversación pueden leer el mensaje
Clave pública y privada	Tu buzón, que se comparte, y su llave, que no
Doble trinquete	Mecanismo que cambia la llave de cifrado en cada mensaje
Remitente sellado	Técnica para que el servidor no sepa quién envía cada mensaje
Metadatos	Datos sobre la comunicación: quién, cuándo y desde dónde
Número de seguridad	Número que comparáis para comprobar que no hay nadie en medio
Poscuántico	Cifrado diseñado para resistir a los futuros ordenadores cuánticos
PIN	Código que protege tu cuenta y permite recuperar tus datos

> **Siguiente paso.** La guía completa, "Signal a fondo", explica cada una de estas piezas con más detalle y sus matemáticas, capítulo a capítulo.

Fuentes: documentación y blog de Signal (signal.org).