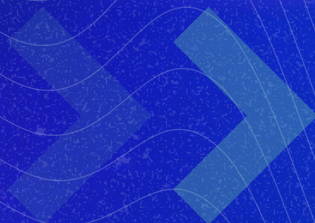


[ESCUELA DE ACTIVISMO DIGITAL]

Tips

PLATAFORMAS Y APLICACIONES MÁS SEGURAS PARA ACTIVISTAS



**Ciudadanía_
Inteligente**



Este cuaderno forma parte de la **Escuela de Activismo Digital** y su objetivo es indicar y analizar algunas aplicaciones y plataformas para Activistas Digitales y explicar algunos términos de tecnología e internet.

Este folleto es una colaboración de la **Fundación Ciudadanía Inteligente con la Informática y Hacker Nina da Hora**.

APLICACIONES DE COMUNICACIÓN

En ninguno de estos usos se utilizan contraseñas que caractericen a la organización o personalicen a algún individuo que forme parte de ella. Es importante no compartir ningún mensaje que contenga contraseñas en estas aplicaciones.



WhatsApp utiliza el cifrado de extremo a extremo, por lo que los mensajes reales son seguros en la plataforma. Pero esto no impide que Facebook abuse de los metadatos: información sobre con quién te comunicas, desde dónde, a qué hora, con qué frecuencia y desde qué dispositivo.

Es bueno de utilizar Whatsapp para listas de transmisión e información genérica e irrelevante.

PARA SABER MÁS

Actualmente una de las cosas más importantes a la hora de elegir una app para intercambiar mensajes es conocer qué seguridad y privacidad ofrece y si de alguna manera la empresa tiene acceso a ella. Pues bien, Facebook compró WhatsApp y en los últimos años han surgido dudas sobre si realmente existe privacidad en los mensajes que se intercambian en la app. En medio de esto es importante buscar alternativas que se adapten a la seguridad y privacidad de la información, aquí hay una lista con pros y contras y algunas estrategias de uso!

El código abierto es otro indicador importante de que un servicio es seguro. Al publicar el código de una aplicación públicamente, cualquiera puede examinarlo para asegurarse de que la aplicación hace lo que se supone que debe hacer. Creemos que el código abierto es uno de los mejores indicadores de que una aplicación es de confianza. Por lo tanto, hemos limitado la siguiente lista de las mejores alternativas a WhatsApp a las aplicaciones de mensajería de código abierto que utilizan el cifrado de extremo a extremo (E2EE). Tenga en cuenta que las aplicaciones no se revisan en ningún orden en particular.



El protocolo de mensajería Signal es un protocolo de mensajería de extremo a extremo, de código abierto, ha sido auditado profesionalmente en cuanto a vulnerabilidades de seguridad y es ampliamente admirado por su fuerza criptográfica. A diferencia de WhatsApp y otras aplicaciones de terceros que implementan el protocolo Signal, la aplicación Signal de la Fundación Signal es 100% de código abierto.

PROS

- Gratis
- Canales para la difusión de mensajes
- Bots para gestionar grupos
- Sincronización entre múltiples dispositivos
- Encuestas, stickers, compartir la ubicación en vivo, gestión de la identidad
- Chat de texto, voz y vídeo con criptografía de extremo a extremo.

CONTRAS

- Requiere un número de teléfono válido para registrarse

PARA SABER MÁS

¿QUE ES CRIPTOGRAFIA?

La criptografía es un conjunto de técnicas diseñadas para proteger la información de forma que sólo el emisor y el receptor puedan entenderla, permitiendo que la información se envíe y reciba de forma confidencial. Prefiera las aplicaciones de mensajería que utilizan el cifrado de extremo a extremo.

El cifrado de extremo a extremo (E2EE) es una función de seguridad que protege los datos durante el intercambio de mensajes, de modo que sólo pueden acceder al contenido los dos extremos de la comunicación.



PROS

- Gratis
- Canales para la difusión de mensajes
- Bots para gestionar grupos
- Sincronización entre múltiples dispositivos
- Encuestas, pegatinas, compartir la ubicación en vivo, gestión de la identidad
- Chat de texto, voz y vídeo

CONTRAS

- Problemas de encriptación
- Sólo los chats secretos son E2EE
- Los chats de grupo (texto o voz) no son E2EE
- No hay chats de vídeo en grupo
- Requiere un número de teléfono válido para registrarse
- Tiene su sede en los Emiratos Árabes Unidos, que no es conocido por los derechos humanos o la privacidad del gobierno (a pesar de tener algunas leyes de privacidad fuertes)



Al igual que Proton, Threema tiene su sede en Suiza, un país con leyes de privacidad de datos muy estrictas e independiente de Estados Unidos y la Unión Europea. También posee su propia infraestructura de servidores en Suiza.

PROS

- No es necesario un número de teléfono o un correo electrónico para registrarse
- Casi no se conservan los metadatos
- Auditoría independiente
- Con sede en Suiza y servidores propios
- Chat de voz y texto en grupo E2EE
- Listas de distribución y encuestas de grupo (sólo para Android)

CONTRAS

- No es gratuito
- Base de usuarios relativamente pequeña
- No hay videollamadas en grupo



PROS

- Gratis
- Creado para la mensajería efímera
- Función anti-censura
- Chat de voz y texto en grupo E2EE
- No es necesario un número de teléfono o un correo electrónico para registrarse

CONTRAS

- Las aplicaciones no son de código abierto
- Las auditorías de seguridad no se publican
- No hay videochat (aunque está disponible en la versión gratuita Pro de la aplicación)

APLICACIONES Y PLATAFORMAS MÁS SEGURAS:

1 GUARDAR LAS CONTRASEÑAS DE FORMA SEGURA

Keepass:

<https://keepass.info/>

Keeper:

https://www.keepersecurity.com/pt_BR/

2 COMUNICACIÓN PARA CONSTRUIR ACCIONES/CAMPAÑAS

Correo electrónico seguro:

<https://mail.riseup.net/>

<https://protonmail.com/>

Lista de correo electrónico seguro:

<https://lists.riseup.net/>

Videoconferencia sin registros:

<https://meet.jit.si/>

Mensajero encriptado - Pidgin:

https://securityinabox.org/pt/pidgin_main

2

Chat seguro a través de Pidgin:

<https://help.riseup.net/en/chat>

SMS seguros con Signal:

<https://whispersystems.org/>

Cliente de correo electrónico cifrado:

<https://emailselfdefense.fsf.org/pt-br/>

https://securityinabox.org/pt/thunderbird_main

Telegram usando el chat secreto:

<https://web.telegram.org/>

3

INTERCAMBIO DE INFORMACIÓN DURANTE LAS SESIONES O ENCUENTROS

Editor de texto colaborativo en línea:

<https://antonieta.vedetas.org/>

Hoja de cálculo colaborativa en línea:

<https://eveliyn.vedetas.org/>

Compartir archivos temporales:

<https://share.riseup.net/>

Compartir texto temporalmente:

<http://oneshar.es/>

4

IDENTIFICACIÓN

Navega por el navegador TOR de forma anónima:

<https://www.torproject.org/>

VPN:

<https://protonvpn.com/>

PARA SABER MÁS

¿QUE ES VPN?

Una **VPN (red privada virtual)** es la forma más fácil y eficaz para que las personas aseguren su tráfico de Internet y oculten su identidad en línea y su ubicación desde donde se conectan. Al conectarse a un servidor de red privada virtual seguro, su tráfico de Internet pasa por un túnel cifrado que nadie puede ver, incluidos los hackers, los gobiernos y su proveedor de servicios de Internet.

5

ALMACENAMIENTO MÁS SEGURO

Creación, almacenamiento, intercambio de archivos y chat:

<https://open365.io>

SpiderOak:

<https://spideroak.com/>

6 PROTECCIÓN

Antivirus, buscador y bloqueo de aplicaciones:

<http://m.onelink.me/164dce10>

Ocultación de fotos y archivos:

<https://archive.codeplex.com/?p=veracrypt>

7 USOS Y APLICACIONES IMPORTANTES PARA LA NAVEGACIÓN

Bloquea la captura de datos del cliente:

<https://prism-break.org/en/projects/privacy-badger>

Bloquear Spams:

<https://github.com/gorhill/uBlock>

Búsqueda anónima:

<https://duckduckgo.com/>

<https://disconnect.me/>

<https://startpage.com/>

Un proyecto de **Ciudadanía_
Inteligente**