EXPOSING THE INVISIBLE

La tecnología es estúpida: Cómo escoger las herramientas digitales adecuadas para trabajar a distancia

Por Marek Tuszynski, cofundador de Tactical Tech

Este artículo recoge los recursos tecnológicos más seguros y adecuados para trabajar de manera responsable desde casa en estos tiempos tan convulsos. ¿Cómo decidimos en qué recursos deberíamos confiar? También habla sobre qué se podría hacer en el futuro para responder a esta pregunta de una forma mucho más sencilla que en el presente.

La tecnología es estúpida, y por eso nos vemos obligados a escribir este texto tan largo al respecto.

Las disyuntivas no suelen ser muy atractivas

En estos tiempos de crisis nos encontramos en una encrucijada tecnológica. Nos enfrentamos a la disyuntiva entre lo rápido y eficaz y lo ético y seguro. En cualquier caso, tenemos que lidiar con las consecuencias políticas y sociales a largo plazo: renunciar a nuestros valores o invertir en unos recursos y herramientas digitales equitativos. Cada vez que ocurre algo que nos obliga a replantearnos el tipo de herramientas de las que disponemos y la manera en la que las empleamos, los socios y el público de Tactical Tech (a través de actividades con participación pública como Glass Room) nos preguntan qué herramientas recomendamos que sean fáciles de usar y funcionales y que no pongan en riesgo nuestra seguridad, privacidad y protección. Dicho de otro modo, suelen pedirnos alternativas a las herramientas que usan con mayor frecuencia. Muchos nos piden que recomendemos herramientas de comunicación, de colaboración y de creación de redes de contactos que estén diseñadas con los derechos y la privacidad de los usuarios como prioridad, y también que funcionen de forma independiente a los grandes grupos que se dedican a recabar datos como Facebook o Alphabet.

Estas cuestiones se han vuelto mucho más comunes durante la pandemia del coronavirus. Se espera que nosotros, o cualquier otra entidad que trabaje en el campo de la tecnología y la sociedad, recomendemos un set de herramientas definitivo, infalible y listo para usarlo. Todo el mundo quiere una lista de herramientas recomendadas, y puede que ni quieran plantearse por qué o por qué no deberían usarlas, y lo cierto es que no son preguntas fáciles. Es una situación urgente, y la gente se preocupa por las decisiones que toma, de modo que al final terminamos sugiriendo alternativas fáciles de usar que requieren menos capacidades, recursos o tiempo. Pero no es —ni debería ser— así de simple. En este artículo hemos recopilado un conjunto de explicaciones, consejos y recomendaciones sobre ciertas herramientas digitales que nos permiten colaborar desde cualquier parte del mundo. También encontrarás muchas sugerencias de lecturas complementarias y te diremos dónde encontrarlas. El texto está organizado en cuatro partes. Te llevará un buen rato leerlo, pero esperamos que merezca la pena.

Primera parte: ¿Qué se esconde detrás de tu pantalla?

La idea de que existen herramientas que siempre le funcionan a todo el mundo, en cualquier contexto, que no requieren conocimientos específicos o infraestructuras adicionales, que son justas y equitativas y que protegen a los usuarios en todo momento, es un sueño que aún no se ha hecho realidad.

Ahora mismo, el panorama no se parece en nada a aquello con lo que soñamos. En los casi 20 años que han transcurrido desde que pusimos en marcha Tactical Tech, hemos visto un cambio considerable: hemos pasado desde herramientas *off-line* que dejan pocos rastros de datos hasta herramientas diseñadas con el único fin de recoger tantos datos personales como sea posible. Por desgracia, la mayoría de las herramientas de las que dependemos hoy las diseñaron empresas con una mentalidad al estilo de Silicon Valley, cuyo modelo de negocio se basa en obtener datos personales.

- *Si no tienes tiempo para leer el libro* La era del capitalismo de la vigilancia, *de Shoshana Zuboff (Paidós, 2020), léete al menos esta entrevista. O también puedes ver este breve documental.*

En Tactical Tech hemos dado con dos métodos para lidiar con el problema del control de datos y la elección de las herramientas digitales: el primero es la mitigación, o «conseguir que sea menos malo». El enfoque de nuestros proyectos Data Detox Kit y Glass Room consiste en ofrecer soluciones rápidas a las necesidades de los usuarios, ya que somos conscientes de que muchas personas, grupos y organizaciones no se encuentran en una posición en la que puedan llevar a cabo cambios drásticos o importantes en las herramientas digitales que emplean. Esto puede deberse a la falta de recursos, capacidades, conocimiento, ayuda o financiación. Estos proyectos están diseñados para adaptarse a ellos e implementar mejoras y cambios progresivos en unos entornos que ya les resultan familiares. Este enfoque no resuelve los problemas, pero sí mitiga algunos de ellos. Ayuda a los usuarios a comprender mejor la tecnología en sí y les ayuda a generar confianza para tomar más decisiones y dar pasos más ambiciosos de cara al futuro.

El segundo método es un cambio de mentalidad que podría llamarse «sufrimiento a corto plazo; beneficio a largo plazo». Cuesta mucho más aplicarlo, y hasta hablar de él resulta complicado. La tecnología sostenible, segura e independiente requiere un cambio considerable en el modo en que la concebimos. Requiere una inversión y unos recursos mucho más significativos, y aunque en Tactical Tech tratamos de promover herramientas gratuitas, de código abierto y alojadas en nuestros propios servidores, sabemos que a muchos de los grupos con los que trabajamos no les conviene. En términos más prácticos, esto exige muchos recursos: puede que las herramientas sean gratis, pero alquilar los servidores o comprarlos no lo es. Mantenerlos tampoco; no puedes depender de voluntarios, y tienes que actualizar tus competencias y recursos de forma constante. También requiere entrenamiento y financiación: si quieres apoyar a organizaciones independientes, seguras, flexibles y sostenibles, hay que pensar tanto en la tecnología como en la gestión, la financiación y los recursos humanos. Este tipo de herramientas son fundamentales para trabajar y necesitan una financiación importante a largo plazo; una financiación que no debería ir dirigida solo hacia los usuarios, sino también hacia los creadores. El motivo por el que algunas de estas herramientas tienen problemas de usabilidad, fallos en el diseño o curvas de aprendizaje muy pronunciadas es porque los equipos que las han desarrollado son pequeños y tienen unos recursos muy limitados. Este segundo método no solo requiere un cambio de mentalidad, sino también un cambio sistémico y tecnopolítico.

Estos dos modelos describen la situación en la que nos encontramos: o nos alimentamos de comida rápida o cultivamos nuestra propia comida. La primera es cómoda, pero no es saludable; y la segunda nos sienta mejor, pero requiere mucho tiempo y habilidades.

¿Es posible construir una sociedad libre, democrática y justa con *software* de código cerrado y privativo (también llamado «propietario»)? ¿Has estado alguna vez en un espacio público que funcione bien y que pertenezca a una empresa? ¿O en una zona común vigilada por cámaras y sensores?

La mayoría de las herramientas digitales que usamos hoy en día no solo funcionan en la nube, sino que se crearon con la idea de que fueran tan sencillas como fuera posible («fáciles de manejar») y que atrajeran al mayor número posible de usuarios («sociales»), que a su vez se volvieran dependientes de las plataformas («basadas en el usuario»). Estas plataformas se ofrecen de forma gratuita (tú eres el producto), mientras que ellas convierten su base de usuarios en una base de datos («*profiling* o elaboración de perfiles») que se puede monetizar (mediante anuncios personalizados o similares). Hacemos clic en «Acepto» para darles acceso a nuestro comportamiento («los metadatos»), y aceptamos las *cookies*, los *beacons* (balizas) y los *scripts*, lo que sea: todo vale, hasta los rastreadores webs (o *trackers*). Una solución posible es instalar algún programa que bloquee la publicidad, pero esos mismos datos se utilizan para darle forma a toda tu experiencia en Internet: los filtros burbuja, los *bots* adaptados a las necesidades de cada uno, los *nudges*, los patrones oscuros (*dark patterns*) y demás. Tu experiencia en Internet es cualquier cosa menos libre y gratis; y por supuesto tampoco es de buena calidad. A estas alturas ya sabemos que hay toda una industria que se dedica a recopilar nuestros datos, pero seguimos usando sus herramientas porque todo el mundo lo hace y es muy fácil confiar en ellas.

Otro aspecto que también deberíamos tener en cuenta es la dependencia. Cualquier caída o interrupción de estos servicios centralizados que usan miles de millones de personas, empresas e incluso gobiernos, provocaría un problema de proporciones épicas. La dependencia a gran escala genera una responsabilidad a gran escala. Ya entrevemos estos escenarios cuando plataformas como Facebook/WhatsApp o Google Docs se caen durante un

breve periodo de tiempo. ¿Qué pasaría si se cayeran durante semanas? Son herramientas como cualquier otra; tienen sus límites y su masa crítica. La cuestión no es si se caerán, sino cuándo lo harán.

Por último, también hay que tener en cuenta sus vulnerabilidades. ¿De verdad es buena idea que el primer ministro de un país como Reino Unido dirija el país desde su casa con una herramienta como Zoom, que no se ha probado, que es privada e insegura? Estos desafíos no conciernen solo a la sociedad civil y a los periodistas de investigación que necesitan confidencialidad y herramientas en las que confiar para mantener su integridad y su seguridad; concierne del mismo modo a los gobiernos, las empresas, las instituciones públicas y los particulares.

Que sean fáciles de manejar quiere decir que se puedan usar sin esfuerzo. En el mundo real, ese esfuerzo, esa resistencia, es necesaria para comprender los sistemas y tomar decisiones, como por ejemplo en el ámbito de las relaciones personales. Por eso mismo, cuando eliminamos el factor de la resistencia en el diseño de las herramientas digitales, es cierto que es más fácil emplearlas, pero perdemos nuestra capacidad cognitiva para entender cómo funcionan y qué modelos de negocio esconden. Este enfoque, combinado con la ludificación (también conocido como «gamificación») de nuestras interacciones (sistemas de recompensas, horas y horas de hacer *scroll*, bucles de *feedback* positivo, etc.), nos vuelve dependientes de unas herramientas que emplean técnicas con las que tal vez no estemos de acuerdo. El escándalo de Facebook y Cambridge Analytica es un muy buen ejemplo de ello.

- Si quieres saber más sobre este nuevo paradigma de los *influencers*, échale un vistazo a nuestro proyecto Data and Politics; en concreto nuestro reportaje «*Personal Data: Political Persuasion*» («Información personal: Persuasión política»).

- Y si te interesa saber cómo se financian estos productos tecnológicos comerciales, puedes empezar por aquí: «*Is Venture Capital Worth the Risk? The industry shaped the past decade. It could destroy next*» («¿Vale la pena el capital riesgo? Esta industria marcó la década anterior. Podría destruir la siguiente»).

Las crisis, y más concretamente una pandemia como la del COVID-19, no solo resultan mortales y peligrosas para la sociedad, la economía y la democracia, sino que también generan un entorno fértil para promover y confiar en modos de actuación autoritarios; y la tecnología siempre resulta muy útil en estos casos. La tecnología dedicada a la vigilancia siempre se promueve en nombre de la seguridad (nacional) y la protección. No es nada nuevo, y ya se ha empleado en otra clase de crisis o como respuesta a otros problemas, como el terrorismo, el control de fronteras o la circulación de refugiados. Ya se puede ver cómo muchas de estas mismas tecnologías (como la geolocalización de los móviles) se emplean como respuesta a la crisis del COVID-19.

- *Aquí puedes echarle un vistazo a la lista de medidas que han adoptado en diferentes países para vigilar a personas en cuarentena. O si prefieres leerlo en el* New York Times, *puedes hacerlo aquí. Échale un vistazo también a cómo se emplea este tipo de tecnología en la crisis fronteriza de la UE en «*Border Troubles: Medical Expertise in the Hotspots*» («Problemas en la frontera: experiencia médica en los puntos conflictivos»).*

Dicho todo esto, en este texto encontrarás varios recursos y referencias. No es la lista mágica que estabas buscando, pero es una forma (más realista) de pensar en las

herramientas digitales que te ayudarán a tomar decisiones informadas y verificables que pueden funcionarte a ti, a tu comunidad y a tu organización. Tienes muchas opciones; el auténtico reto no es solo escoger una u otra, sino también pensar qué tipo de sociedad estamos apoyando cuando tomamos esas decisiones.

Segunda parte: Lo que funciona y lo que no

Unos cuantos principios útiles para escoger las herramientas digitales

Estos son algunos de los principios que siempre han guiado las decisiones que tomamos en Tactical Tech a la hora de escoger las herramientas que usamos; también te ofreceremos algunas recomendaciones concretas. La idea es darte un marco de referencia que te ayude a encontrar las respuestas adecuadas a tus necesidades, pero que también se ajuste a tus capacidades y recursos. Si no estás de acuerdo, siempre puedes tomar tus propias decisiones, que seguramente te resultarán más convenientes (y es posible que tu respuesta sea Google Workspace o WhatsApp /Facebook); todo depende de lo que sea más importante para ti.

Siempre intentamos seguir estos siete principios a la hora de escoger herramientas digitales. Tienen que:

1. Ser de código abierto;
2. Ser de confianza (es decir, que se hayan revisado);
3. Llevar tiempo en funcionamiento (que sean estables, que tengan una comunidad de usuarios activa y una comunidad de desarrolladores responsable);
4. Ser fáciles de usar;
5. Estar disponibles en varios idiomas y contar con un soporte de localización (para que puedas usarlas o en tu propio idioma o localizarlas);
6. Estar disponibles para varias plataformas (Mac, Windows, Linux, Android);
7. Tener la documentación al alcance de cualquiera.

    - *Si crees que nos hemos olvidado de dos aspectos fundamentales (es decir, los datos y el cifrado), ¡tienes razón! Los hemos dejado para más adelante. Por otro lado, en lo que respecta al primer punto, preferimos emplear* software *libre y de código abierto (Free Libre Open Source Software, o FLOSS); sin embargo, nos ceñiremos al término «código abierto» para evitar usar el*

término «free», ya que se confunde a menudo con el freeware (sin coste por licencia), freemium (servicios gratuitos con características adicionales de pago) o software *propietario gratis, y no nos referimos a ninguna de esas cosas*

Los siete principios de arriba pueden resumirse en una única idea: **nos basamos en la confianza.**

Dado que el *software* se desarrolla mediante códigos, queremos confiar en su código y no en las promesas de quienes quieren que lo utilicemos. Si puedes elegir entre una caja negra (*software* propietario) y una caja blanca (*software* de código abierto), elige siempre la blanca. Recomendar o confiar en una caja negra es arriesgado porque tienes que creerte a pies juntillas todas las promesas de los fabricantes. Las personas ajenas a la empresa no saben si el código que han empleado es bueno o malo. De hecho, no sabemos casi nada de los datos qué recogen, adónde van, etc. Esto no quiere decir que el código abierto sea siempre mejor; de hecho, también es solo un código que han programado varias personas y que conlleva sus propios riesgos. Pero, como es abierto, puede verificarse, y eso es fundamental. Algo que también cabe destacar sobre el código abierto es que lleva una licencia libre, por lo que los usuarios pueden desarrollar la herramienta de forma independiente, compartirla con terceros o modificarla. Y es gratis.

Por desgracia, la expresión «código abierto» se ha empleado hasta la saciedad para describir el *software* y se ha vuelto un poco confusa. Es posible que algunos componentes sean de código abierto (por ejemplo, una aplicación que puedes usar en tu dispositivo), pero puede que el *software* que se ejecuta en el servidor de la empresa (la nube) sea de código cerrado.

En cuanto al resto de principios, lo que está claro es que en tiempos de crisis se produce una necesidad sin precedentes de soluciones rápidas. Y no solo por parte de usuarios particulares, sino también por parte de inversores, empresas, gobiernos, etc. Al mismo tiempo, son tiempos en los que pueden producirse toda clase de innovaciones. Pero, al igual que todo lo que ocurre durante una crisis, suele resultar caótico. Las peticiones centradas en resolver problemas a corto plazo generan soluciones que provocan otros problemas. Apenas hay tiempo para llevar a cabo pruebas, eliminar errores y comprender siquiera qué está ocurriendo. Es por ello que creemos que, a la hora de escoger qué herramienta usamos, es importante que lleve bastante tiempo en funcionamiento. Puede que parezca un enfoque demasiado prudente —y seguramente lo sea—, pero también es responsable y racional, porque las decisiones precipitadas tienen consecuencias reales a largo plazo. Además, quienes las sufren suelen ser quienes más protección y atención necesitan.

- *Para obtener una lista y una explicación detallada de estos principios, visita el proyecto Security In-A-Box (Seguridad en una caja) que creó Tactical Tech y que luego desarrolló en conjunto con Frontline Defenders. Busca la sección sobre los criterios de selección.*
- *Y si eres un defensor de los derechos humanos que trabaja a distancia, lee la guía de Front Line Defenders «Protección física, emocional y digital para el trabajo desde casa en tiempos del COVID-19: Ideas y consejos para personas defensoras de los derechos humanos».*

Tercera parte: algunas herramientas básicas recomendadas

Aquí, por fin, te presentamos la parte que tanto esperabas: algunas de las herramientas que recomendamos y utilizamos porque siguen los principios de los que hemos hablado. Es posible que incluso ya uses algunas de las esenciales. También esperamos que tengas el sistema operativo actualizado, al igual que todas las aplicaciones… Es más fácil decirlo que hacerlo.

Para organizar la comunicación en línea desde tu dispositivo

Los navegadores de Internet que recomendamos

- Tor Browser
- Firefox
- Chromium
- Brave

Los complementos que recomendamos

Es imprescindible escoger el motor de búsqueda adecuado para que sea el predeterminado e instalar unos cuantos complementos. Como mínimo estos:

- HTTPS Everywhere
- uBlock Origin
- Facebook Container

Correo electrónico

- Thunderbird

Gestores de contraseñas

- KeePassXC
- Si tienes que utilizar una herramienta en línea, prueba Firefox Lockwise

Mensajería instantánea

- Signal

Almacenamiento seguro de archivos

- Veracrypt
- Cryptomator

Conectarse a Internet de forma segura. VPN gratuitas

- Riseup VPN (gratuito)
- Proton VPN (gratuito)
- Psiphon (gratuito)
- Lantern (gratuito hasta 500 MB)
- TunnelBear (gratuito hasta 500 MB, no es de código abierto, bueno para principiantes)

También existen muchas opciones de pago estupendas y, a menos que puedas configurar tu propia VPN, te recomendamos encarecidamente que les eches un vistazo. Pero nunca utilices una VPN comercial gratuita; obtienen beneficios recopilando datos. Si quieres saber más sobre las VPN, te recomendamos que le eches un vistazo a «Escogiendo el VPN apropiado para usted» en EFF.

Aquí y aquí puedes consultar una lista detallada de VPN de pago acompañadas de una descripción general. Y si aún quieres saber más sobre cómo hacer que tus comunicaciones sean privadas, léete otro capitulito de Security in a Box (Seguridad en una caja).

La nube: no es oro todo lo que reluce

Recuerda que, a efectos prácticos, «la nube» es el ordenador de otra persona. Hay nubes enormes (de *software* privativo), que pueden ser servidores que están a tu disposición para ejecutar servicios (Amazon, Microsoft) o plataformas que almacenan y procesan tus datos (Facebook, Alphabet o sus filiales, como Instagram, Google Maps, Zoom, Slack y muchas más). También existen nubes de un tamaño mediano gestionadas por operadores relativamente pequeños que pueden tener una infraestructura propia, pero que proporcionan servicios especializados (de código abierto, por ejemplo, Greenhost) o lo que necesites, pero dependen de las nubes grandes que ya hemos mencionado. Por último, también hay nubes pequeñas, nubes alojadas en servidores propios (en su mayoría, de código abierto, sobre el que se tiene el control) puestas en marcha por instituciones, organizaciones o particulares.

No todas las nubes son iguales. En Tactical Tech preferimos usar las pequeñas y las medianas que respetan los derechos y las libertades de los usuarios, y también aquellas que dependen de sistemas de código abierto con modelos de negocios que no se basan en monetizar datos.

«La nube», como concepto, es algo muy valioso: le permite a una multitud de usuarios (mediante ordenadores portátiles y teléfonos móviles) ampliar el abanico de posibilidades. Tu navegador y las aplicaciones de tu teléfono se convierten en la interfaz de un sistema más potente y eficaz que te ofrece herramientas y contenido desde un lugar remoto (suponiendo que seas lo bastante privilegiado como para tener una conexión a Internet rápida y barata). Te permite llevarte los datos a cualquier parte; puedes acceder a ellos desde diferentes dispositivos y lugares, y puedes compartirlos con facilidad.

Ese no es el único modelo disponible. Nuestros dispositivos pueden llevar a cabo muchas de las actividades que dependen de la nube (compartir documentos, por ejemplo), y nos permiten hacer muchas cosas entre nosotros. Es lo que se conoce como «red de pares» (o red P2P, por sus siglas en inglés). Un ejemplo de ello es BitTorrent, una plataforma de intercambio de archivos. Muchas empresas de videojuegos de ordenador (como el Diablo III, StarCraft II y World of Warcraft) distribuyen sus productos a través de redes de pares. Otros ejemplos son Tor, la herramienta dedicada al anonimato, y Bitcoin, la criptomoneda, que puede que hoy en día sean las redes de pares más conocidas. Los usuarios necesitan sistemas que no estén centralizados, que permitan la interoperabilidad y la comunicación entre pares y que no requieran una estructura central excesiva y cara.

Hoy en día cualquiera que tenga un ordenador portátil o un teléfono inteligente depende de un modo u otro de los servicios de la nube. Hay quienes lo hacen casi todo en la nube (en las grandes). Ofrecer recursos y servicios en la nube supone una fuente de ingresos inmensa para casi todas las empresas que se dedican al sector de los datos, como Alphabet, Apple, Amazon, Facebook, Microsoft y Netflix, por mencionar algunas de las más grandes. Pero las empresas como Uber y Zoom siguen el mismo modelo. Ellos gestionan la infraestructura y recaban todos los datos posibles. Lo que nosotros vemos es la interfaz de esa infraestructura centralizada y nos beneficiamos de unas herramientas eficaces; y a cambio perdemos todos los datos que van a parar a ese sistema y que se van acumulando. Además, también renunciamos al conocimiento acumulado, y puede que esto sea lo más importante para la sociedad

En el ámbito de los datos, es mejor decantarse por el minimalismo. A la hora de usar y escoger los servicios de una nube, intenta buscar los recursos y las herramientas que recaben y compartan los menos datos posibles y que almacenen la menor cantidad de datos esenciales. Si eres tú el que tiene que ofrecer algún servicio, ya sea organizar un evento, mantener una lista de correo o hacer una encuesta, y no te hace falta recabar datos, no lo hagas. Si tienes que hacerlo, sé claro y transparente, minimízalo en la medida de lo posible y borra todo lo que ya no necesites.

- *Si no te queda más remedio que utilizar Facebook y otras plataformas populares, el Data Detox Kit de Tactical Tech ofrece una serie de pasos sencillos para ayudarte a tener un mayor control sobre tu privacidad digital, tu seguridad y tu integridad mientras utilizas tus dispositivos y plataformas preferidos.*

Creemos que ayudar a los usuarios a ser conscientes de lo que ocurre detrás de las pantallas de sus dispositivos, sin importar qué plataformas empleen, es un paso muy importante para

poder tomar decisiones informadas y comprender tanto las políticas que hay detrás de las herramientas digitales como la repercusión que tienen en nuestra vida.

- *Si utilizas o recomiendas Slack, Zoom u otras herramientas en línea para trabajar, aprender o proporcionar o recibir servicios sanitarios, por favor, lee esto: «Lo Que Debe Saber Sobre las Herramientas Online Durante la Crisis de COVID-19».*
- *Y si eres activista y usas las redes sociales, lee la guía* Activism on Social Media: A Curated Guide.

La importancia del cifrado

Aunque recomendamos las herramientas en línea o en la nube según los principios que ya hemos mencionado, también tenemos que evaluar otros aspectos que garanticen la confidencialidad y la seguridad de las comunicaciones, como el cifrado de extremo a extremo. ¿Qué es el cifrado de extremo a extremo? Es la tecnología que nos permite enviarle un mensaje a otra persona de modo que solo tú y ella podáis leerlo. Si alguna otra persona tiene acceso a dicha conversación, tan solo verá un sinsentido; sin embargo, sí pueden ver los metadatos (suelen ser los proveedores del servicio quienes lo hacen), es decir, que pueden ver que estás enviando mensajes, desde dónde los envías, cuándo, con qué frecuencia y a quién se los mandas. Lo único que no pueden ver es el contenido de los mensajes.

Existen muchos servicios diferentes que emplean el cifrado. Gracias a él podemos llevar a cabo tareas sencillas en la red, como por ejemplo acceder a la banca electrónica o comprar por Internet, de forma segura y confidencial. Algunos servicios de comunicación les prometen a sus usuarios que emplean el cifrado de extremo a extremo, pero en realidad tan solo cifran la información que circula entre ellos y sus servidores, y entre sus servidores y el destinatario de los mensajes, pero esos servidores tienen acceso a toda la información sin cifrar. Por lo tanto, tu información solo está cifrada cuando está en movimiento, pero, técnicamente, no está protegida del proveedor del servicio, que puede acceder a ella, procesarla, analizarla o reutilizarla.

El cifrado de extremo a extremo tiene algunos límites. A veces las empresas afirman que lo utilizan, pero para un usuario medio puede ser complicado comprobarlo. Algunos de estos servicios son opcionales, y otros solo son parciales. En algunos el cifrado solo puede funcionar hasta cierto nivel; por ejemplo, en las conversaciones entre dos personas, pero no en los chats grupales. O puede que funcione correctamente cuando se usa un servicio de una forma concreta (en tu iPhone, por poner un ejemplo), y que no funcione en otros servicios relacionados, por ejemplo, en las copias de seguridad. Todo esto hace que a los usuarios les resulte complicado navegar y tomar buenas decisiones sin comprobar todos los detalles.

- *Si quieres saber más sobre el cifrado de extremo a extremo o cómo funciona, te dejamos por aquí una explicación muy sencilla y muy útil de la EFF.*

En tiempos de crisis, el cifrado se convierte en un tema de debate. Cada vez que se analiza la delincuencia en Internet, la desinformación o los fraudes, parece que el cifrado forma parte del debate, y hay quien afirma que hace posibles estos delitos y actividades ilícitas. Está claro que existe cierta correlación, pero la causalidad es mucho más compleja. Pongamos el caso

de que un terrorista decide emplear un coche como arma; esto no hace que todos los coches sean armas de terrorismo. Siguiendo esa misma lógica, que el cifrado se utilice para una actividad criminal no quiere decir que el cifrado en sí sea un delito. WhatsApp es un buen ejemplo de ello porque cifra las conversaciones de sus usuarios, pero recaba los metadatos (como ya hemos explicado antes). WhatsApp cuenta con aproximadamente dos mil millones de usuarios, y el hecho de que ni siquiera WhatsApp pueda leer esas conversaciones tiene sus ventajas. El cifrado hace posible la comunicación (puede que yo, por ejemplo, no tenga nada que esconder, pero eso tampoco quiere decir que tenga por qué mostrarte todas mis conversaciones) y (por ahora) la protege de la publicidad personalizada basada en el contenido de las conversaciones (aunque Facebook siempre está buscando formas de monetizar su base de datos de los usuarios, así que quién sabe qué puede pasar en el futuro).

Quienes se muestran más escépticos con el cifrado creen que este es la causa principal de la desinformación. Dado que el cifrado permite el secretismo, hay quien cree que es un canal seguro para organizar delitos (lo cual es muy cierto: el cifrado ofrece confidencialidad, seguridad *y* secretismo; todas estas cosas van de la mano), pero eso depende exclusivamente de los usuarios. Hay que tener en cuenta muchos más matices. La escala del canal cifrado es lo que permite que circule la desinformación dañina. Lo que permite que la información errónea se difunda son las acciones de los usuarios. Es cierto que las redes criminales y demás delincuentes se aprovechan del cifrado, pero si WhatsApp lo elimina, lo más seguro es que empiecen a utilizar alguna otra herramienta.

Todo esto no quiere decir que el cifrado sea algo malo. Como pasa en muchos casos, la tecnología no es buena ni mala; **la tecnología es estúpida, pero nunca neutral.** Todo depende de las intenciones de quienes la usan. Puede que el problema vuelva a ser el modelo de negocio. Al escoger casi siempre estas herramientas para comunicarnos a gran escala, apoyamos unos sistemas monolíticos centralizados que operan a nivel mundial y que provocan problemas mundiales.

- *Este tema tiene muchos matices, como por ejemplo la difusión multiplataforma de la desinformación (pese al cifrado) y la responsabilidad de los usuarios. Échale un vistazo a este artículo reciente sobre el tema para leer un análisis más profundo sobre WhatsApp y la desinformación.*

En resumen, estas son algunas de las cosas que debes recordar:

- Averigua cuál es el modelo de negocio de la herramienta que estás usando. ¿Cómo monetizan el uso gratuito?
- Léete los términos y condiciones y las políticas de privacidad (sí, ya lo sabemos…, pero tienen la obligación de explicarte cómo funcionan).
- Piensa qué nube es la más adecuada para ti (grande, mediana o pequeña) y plantéate si puedes permitirte un servidor propio.
- Busca herramientas que aboguen por el minimalismo de datos.
- Vuelve a comprobar qué tipo de cifrado (de extremo a extremo/en tránsito) emplean.

Recomendaciones de herramientas en línea

Convirtamos esos principios en algunas recomendaciones:

Comunicación entre dos personas o en grupos pequeños: llamadas de voz y mensajería

- Signal
- Wire (tanto Signal como Wire pueden alojarse en un servidor propio, pero no resulta sencillo, ya que habría que crear versiones dedicadas de las diferentes aplicaciones cliente)
- Riot, una interfaz para matrix (para usarla tienes que habilitar la encriptación por sala de chat, y la verificación por clave resulta compleja desde la perspectiva del usuario; también puedes alojarla en un servidor propio).
- Como alternativa a Riot, recomendaríamos echarle un vistazo a Mattermost, que ofrece diferentes opciones de alojamiento y desarrollo.

Para saber más sobre por qué preferimos Signal a WhatsApp, consulta este post. Si te interesa el uso de WhatsApp en el contexto actual, puedes leer esta entrevista con Stephanie Hankey, de Tactical Tech.

Comunicación para grupos más grandes: llamadas de voz y vídeo

Para las conversaciones de voz y vídeo en grupo recomendamos utilizar Jitsi Meet. Puedes utilizarlo desde sus servidores o hacerte con el *software* y ejecutarlo en tu propio servidor.

Jitsi no es un servicio único, sino una herramienta que puede ejecutar cualquier persona en cualquier lugar, por lo que se pueden usar muchas instancias («*instances*», en inglés; redes virtuales que te permiten comunicarte de forma segura con otros miembros de tu organización), a diferencia de herramientas como Skype o Zoom. Algunos de los servidores de Jitsi que puedes utilizar son:

- Greenhost
- Collective Tools
- Disroot
- *Aquí tenéis una lista enorme de instancias disponibles para Jitsi Meet. Hay que recalcar que Jitsi Meet ofrece cifrado de extremo a extremo solo para las llamadas entre dos personas (esta es la limitación a la que se enfrenta este tipo de videoconferencias y audioconferencias en navegadores con varias personas). Puedes usarlo con más personas, pero tienes que confiar en el anfitrión. Esto no es algo exclusivo de Jitsi Meet: la mayoría de las herramientas disponibles ofrecen un cifrado de extremo a extremo solo para videollamadas con muy pocos participantes. Pero se pueden reducir los riesgos utilizando el cifrado en tránsito y asegurándote de que el servidor que se usa de intermediario es de confianza.*

En nuestra experiencia, Jitsi Meet funciona bien con grupos pequeños (diríamos que hasta ocho o diez personas) y luego las cosas se complican un poco. Además, exige muchos recursos a los dispositivos de los participantes, tanto de capacidad como de batería. Dicho esto, nosotros utilizamos Jitsi muy a menudo. Si necesitas un entorno parecido al de una clase, con pizarra, muchas salas, chat, voz y vídeo, así como la posibilidad de compartir la pantalla, presentaciones y vídeos externos, te recomendamos que utilices BigBlueButton, sobre todo para quienes puedan alojarlo en un servidor propio. Es ideal para reuniones de

equipos y seminarios web, ya que también permite participantes externos. Soporta más participantes que Jitsi Meet, y a los usuarios que se unan solo les hace falta un navegador.

Si crees que Zoom tiene una encriptación de extremo a extremo, estás equivocado; ofrecen encriptación de transporte, lo que significa que todo lo que haces en Zoom puede desencriptarse fácilmente en sus servidores. Este es uno de los problemas de esta herramienta (junto con algunos otros que comentaremos al final).

Entendemos que tal vez necesites hablar con más gente al mismo tiempo, sobre todo si intentas llevar a cabo conferencias o cursos *online*, pero de momento Zoom tiene demasiados problemas que debe resolver, y todos seguimos buscando alternativas viables. Como mínimo, piensa en utilizar otros servicios o, si puedes, divide tu trabajo en partes. ¿Puedes transmitir en directo algunas de las partes? ¿Puedes organizar un seminario web y pregrabar parte del contenido? ¿Puedes reducir las partes interactivas de tu trabajo para adaptarlas a varios grupos más pequeños o utilizar varios canales (por ejemplo, un canal para documentos colaborativos y otro solo para el chat de voz, como Mumble)?

Puesto que no disponemos de las herramientas perfectas, es posible que tengamos que ser más creativos a la hora de diseñar colaboraciones virtuales según las necesidades.

Alojamiento de vídeos

Por último, para el alojamiento de vídeos, utilizamos principalmente Vimeo, aunque no cumple nuestros criterios (no es de código abierto y han salido a la luz varios problemas recientes). Hoy en día estamos experimentando también con el alojamiento en nuestros propios servidores a través de PeerTube.

Colaboración

A la hora de colaborar, para actividades como compartir calendarios, editar documentos y compartir archivos, recomendamos Nextcloud.

Al igual que con Jitsi, puedes probarlo desde sus servidores, pero si quieres utilizarlo tendrías que alojarlo en uno propio o encontrar un proveedor que lo aloje por ti. Si no es posible utilizar un servidor propio, recomendamos usar herramientas distintas para cada propósito.

Compartir archivos

- RiseUp Share;
- OnionShare;
- *Si buscas una alternativa a WeTransfer o Hightail prueba Tresorit Send, pero ten en cuenta que no es de código abierto.*

Compartir calendarios

- Tutanota, un servicio de correo que también ofrece un calendario cifrado.

Trabajar juntos en documentos

- RiseUp Pads;
- CryptPad, que también se puede alojar en servidores propios;
- *Si estás pensando en una alternativa descentralizada a Google Docs, olvídate. Nos encantaría recomendarte alguna, pero lo cierto es que no la hay.*

Gestión de proyectos

Si buscas una forma independiente de gestionar proyectos y estás dispuesto a invertir en infraestructura y conocimientos, entonces te recomendamos usar Gitlab alojado en un servidor propio, que es adecuado para personas con diferentes niveles de habilidades técnicas.

Va bien para gestionar equipos grandes, proyectos complejos que requieren tareas distintas, listas de tareas, comentarios, cuestiones o edición de texto básico. Si puedes alojarla en un servidor propio y no te importa aprender un poco sobre cómo usar una herramienta que en realidad se creó para gestionar programaciones, es una muy buena opción. Si no, también puedes usar Nextcloud, que ya la hemos mencionado antes, con complementos como «deck».

- *Cuando te plantees qué herramientas podrías necesitar para comunicarte y colaborar con tu equipo, puedes ver la conferencia de Julian Olivier de 2019, en la que explica el proceso de configuración de un entorno firme y fiable para Extinction Rebellion llamado «*Server Infrastructure for Global Rebellion*» («Infraestructura de servidores para la rebelión global», en español).*

Cuarta parte: alejémonos un poco y pensemos a largo plazo

Es fundamental que, cuando propicies una colaboración con otras personas y propongas usar ciertas herramientas, tengas en cuenta algunos factores. Primero: en Internet, no todo el mundo es igual. La persona con la que te comunicas puede tener muy limitado el acceso a Internet, o puede que le resulte muy caro o que la cantidad de datos que puede utilizar para una transferencia sea muy limitada (envíar vídeos consume muchos datos). Segundo: es posible que sus dispositivos estén desfasados o que no sean seguros, o puede que los compartan con otras personas. Tercero: su entorno

social, económico y político puede ser mucho menos seguro y predecible. Puede que esté poniéndose en una situación de riesgo solo por el hecho de exponer sus vulnerabilidades, su estado, sus visitas, sus creencias o sus asociaciones al comunicarse contigo. Solo por que tú puedas hacer algo, no quiere decir que los demás tengan que hacer lo mismo. Piensa muy bien en las decisiones que obligas a tomar a otras personas cuando las invitas a participar en tus actividades.

Si quieres más detalles, envíanos un correo para pedirnos el informe de investigación que publicaremos en Tactical Tech (ttc@tacticaltech.org)

Si estás en Internet, te están rastreando

Te están rastreando antes de que abras siquiera tus aplicaciones favoritas. Así es cómo funciona la telefonía móvil para proporcionar sus servicios. La telefonía móvil funciona porque nuestros teléfonos siempre están geolocalizados; así las operadoras siempre aseguran que haya buena cobertura para que podamos hacer llamadas y tener datos en todas partes. Esa información les basta para determinar nuestro paradero, y esa información se acaba convirtiendo en datos de comportamiento (dónde vivimos, cómo nos desplazamos, con quién interactuamos y qué nos interesa).

- *Tactical Tech creó este vídeo hace tiempo para mostrar todo lo que se puede saber a partir de los datos que recogen los teléfonos móviles.*

¿Por qué es tan importante esto hoy en día? Estamos viendo que, en muchos lugares, las teleoperadoras utilizan y comparten los datos que recaban de los teléfonos con gobiernos e instituciones públicas para rastrear, vigilar y contener la expansión del coronavirus, pero también para comprobar qué parte de la población permanece en casa y para asegurarse de que lo hagan. Los artículos sobre este tema surgen a diario por todo el mundo; por ejemplo, en Austria y Alemania. Otros gobiernos colaboran con empresas de inteligencia, como Palantir en el Reino Unido. O emplean herramientas fabricadas por empresas como NSO, conocidas por recabar información confidencial y *hackear* a los ciudadanos.

- El escándalo de Cambridge Analytica (https://es.wikipedia.org/wiki/Cambridge_Analytica) destapó el uso de la publicidad personalizada y el perfilado (*profiling*) psicológico (dos métodos que se han empleado durante años pero que solo conocían quienes lo usaban para lucrarse. Con suerte, el uso de macrodatos (o *big data*) de geolocalización para rastrear y contener la expansión del coronavirus expondrá algo que siempre ha estado presente: que los teléfonos móviles son rastreadores. Estos datos se vuelven más detallados y precisos cuando hablamos de teléfonos inteligentes que cuentan con localizador de redes y GPS.

Junto al término «macrodatos» solemos escuchar otra palabra mágica: «anonimización»

La anonimización es un proceso a través del cual se separan los datos de la identidad del usuario. Esto quiere decir que es posible que veas mis datos (qué me gusta comer o cada cuánto cojo un taxi), pero no sabes quién soy. Por desgracia, la anonimización es muy parecida al concepto de «seguridad». Son aspiraciones, y no estados permanentes que podemos alcanzar. La seguridad es un proceso continuo que requiere mantenimiento. La

anonimización es un proceso que ofrece un poco de protección a los usuarios y a las empresas que recaban sus datos. Sin embargo, con paciencia y los conjuntos de datos suficientes, estos procesos pueden deshacerse. No sería la primera vez que se hacen públicos varios conjuntos de datos y se desanonimizan para revelar información comprometedora sobre los usuarios (puedes verlo aquí)

- Tactical Tech ha creado este vídeo para explicar cómo funciona la anonimización

Los problemas colectivos requieren soluciones colectivas

La sociedad civil no dispone de herramientas digitales fiables y consistentes que protejan la privacidad de los usuarios porque casi nadie invierte en ese tipo de herramientas; ni los inversores ni los gobiernos ni los financiadores privados. Paradójicamente, ellos son los primeros en pedir recomendaciones y quejarse de que las herramientas que se les ofrecen no satisfacen sus expectativas, y nunca lo harán. La tecnología es fundamental para los particulares, las organizaciones, el conjunto de la sociedad civil y la esfera pública. Es una verdadera pena que tengamos que depender en exclusiva del sector privado, un sector cuyas decisiones vienen motivadas por la obtención de beneficios. Hoy en día, la mayoría de herramientas que usamos vienen de EE. UU. Las principales alternativas vienen de países como China (TikTok ya tiene un alcance mundial) y Rusia (Yandex, el motor de búsqueda regional). El modelo de negocio de casi todas estas opciones se basa en obtener beneficios de los datos personales.

La tecnología cuesta dinero (y mucho); no solo para crear las herramientas, sino para su mantenimiento, lo que puede ser incluso más importante. La infraestructura que necesitan para operar es aún más cara, y las habilidades que requieren sus creadores y administradores son fundamentales. Si queremos que las organizaciones cuenten con herramientas duraderas en las que puedan confiar, tienen que tener acceso a los conocimientos técnicos y a los recursos para alojar los servicios que necesitan en servidores propios, o disponer de alternativas que funcionen a gran escala. A día de hoy, esto aún no ocurre.

Ya no basta con unirse a quienes no utilizan Facebook, evitan Google o hasta se instalan sistemas operativos personalizados (ROM) en sus teléfonos móviles, o tan solo confían en el código abierto (seamos sinceros: a algunos de nosotros en Tactical Tech también nos pasa). Hace falta una solución colectiva; no una que intente volver al pasado, cuando los datos no eran un activo valorado en miles de millones de dólares, sino una que mire hacia el futuro. Nos encontramos en un momento importantísimo para aprender qué tienen de malo las opciones que tenemos y qué repercusiones tienen estas prácticas en diferentes sectores (como el de la educación) en las comunidades que los necesitan y en el conjunto de la sociedad. Es el mejor de los tiempos para reevaluar qué herramientas necesitamos y por qué las necesitamos, y también para ser innovadores y crear alternativas viables que funcionen en aras del interés público.

Para enfrentarnos a una pandemia tenemos que colaborar, ser solidarios y establecer redes de contactos. Hace falta ciencia de buena calidad y una buena toma de decisiones. Todas estas respuestas tienen que apoyarse en la tecnología o aprovecharla para maximizar su potencial. Ha llegado la hora de decidir en qué bando estás.

Casi todo este texto se centra en las necesidades de las personas y de los grupos pequeños y en las herramientas digitales que pueden emplearse en tiempos en los que se ha aumentado el

trabajo a distancia. Cabe destacar que los problemas que hemos expuesto en este texto son aún mayores cuando hablamos de instituciones y organizaciones de mayor envergadura: fundaciones, universidades, colegios, hospitales, organizaciones humanitarias, redes formales e informales, etc. Todas estas instituciones han tenido que pasar a funcionar de manera virtual de la noche a la mañana. Ahora mismo están tomando decisiones cruciales sobre plataformas, proveedores, servicios, herramientas y aplicaciones sin apenas tiempo para poder formarse en cómo se utilizan y a menudo sin financiación adicional. Tienen que contemplar los recursos, las obligaciones, las expectativas y las exigencias. Trabajar en estas condiciones es dificilísimo. Y la eficacia vuelve a ser muy importante, y suele serlo más que otros aspectos. A nivel institucional (y también a nivel personal) resulta complicado imaginar un mundo en el que Microsoft, Google y Zoom no sean de ayuda para los colegios e institutos. Estos servicios ayudan a que los centros puedan funcionar virtualmente de una manera más eficiente y barata, pero también hace que padezcan los mismos problemas que hemos comentado sobre las plataformas que funcionan a gran escala y las desventajas que conllevan todas sus ventajas. Para imaginar herramientas digitales alternativas tenemos que imaginar tecnopolíticas alternativas (como quién recaba los datos, cómo lo hace y quién se beneficia) y modelos de negocio alternativos… ¿Qué pasaría si se emplearan los ingresos tributarios para crear herramientas digitales de buena calidad?

- *Si quieres leer más sobre los problemas que conllevan los recursos tecnológicos, puedes echarle un vistazo a este ensayo: Efficiency and Madness (*Eficacia y locura, *en español).*

No es que estemos trabajando o asistiendo a clase a distancia como si no pasara nada. Intentamos trabajar, estudiar y hacer cosas importantes en medio de una crisis sanitaria tremenda. Nadie sabe cuánto durará, pero sabemos que afectará a otros aspectos de nuestra vida y que cambiará nuestro modo de hacer las cosas, tanto a nivel doméstico como profesional, social, económico, político y demás. Las decisiones que tomen ahora las instituciones, las organizaciones, los gobiernos y los individuos definirán el modo en que trabajaremos en el futuro.

Todavía no hemos visto herramientas desarrolladas con la mentalidad de Silicon Valley para estos propósitos. No podemos dejar que la inmediatez del coronavirus nos ciegue ante las consecuencias a largo plazo y nos veamos atrapados en unas herramientas que no funcionan según las necesidades de la sociedad civil.

El cielo está despejado y los pájaros cantan más fuerte que nunca

Aprovechemos también estos tiempos para reflexionar y recapacitar. Es probable que esta pausa, este encierro, este distanciamiento, dure bastante en diferentes lugares. Aún no sabemos lo grave que será. En algunos casos, otorgará más poder a los regímenes autoritarios y las empresas que los propician. Sin embargo, también podría ser un momento de claridad, reconocimiento, solidaridad y colaboración, de modo que cuando superemos esta etapa habrá mucho que hacer. Puede que ahora tengamos buenos motivos para dedicar tiempo, invertir dinero y encontrar el apoyo para hacerlo.

La tecnología es estúpida, los teléfonos inteligentes son estúpidos y la inteligencia artificial también. La pregunta es: ¿cómo de listos somos nosotros?

Recursos relacionados que te recomendamos para empezar

Un enfoque holístico

Como afirma la guía de Holistic Security: «La seguridad es un concepto personal y subjetivo, y depende también del género. Cuando trabajamos para lograr un cambio social positivo, podemos enfrentarnos a amenazas y ataques persistentes que pueden afectar a nuestros amigos y familias, y menoscabar nuestra integridad física y psicológica». Sin embargo, ser organizado en lo que a seguridad se refiere nos puede ayudar a preservar nuestra salud y nuestro trabajo. Puedes encontrar más información aquí y en la gran comunidad de seguridad holística.

El género y la tecnología

La colaboración, las interacciones y las comunicaciones en línea son especialmente peligrosas para las mujeres, los grupos minoritarios y quienes ponen en práctica sus libertades fundamentales en entornos restrictivos y antidemocráticos. A través de varios talleres y colaboraciones, Tactical Tech cocreó una serie de estrategias, métodos y guías que a día de hoy sigue usando y manteniendo una comunidad más amplia. Aquí puedes encontrar una wiki y un programa de formación con el que aprenderás cosas como:

- Servicios de alojamiento web autónomos y éticos;
- Cómo escoger a tu proveedor de servicios;
- Estrategias de comunicación feministas;
- *Hackear* discursos de odio:
- Cómo funciona Internet;
- Y más veinte temas distintos.

En el caso de que estés desarrollando herramientas digitales y hayas llegado hasta aquí…

Si eres desarrollador, diseñador de sistemas, ingeniero, alguien que se está planteando montar una empresa, organizar un *hackatón* o que quiere poner a prueba sus habilidades, léete el «*Critical Engineering Manifesto*» («Manifiesto del Ingeniero Crítico», en español), que sigue siendo relevante a día de hoy, y mucha suerte cuando te pongas a programar.

También puedes ver cómo lo hacen otros en:

- Por ejemplo, el Guardian Project;
- O puedes ver otros proyectos respaldados por el Open Technology Fund, siempre que no te importe que estén financiados por el congreso de los Estados Unidos (a nosotros no nos importa, ya que las herramientas que apoyan son de código abierto y están localizadas y auditadas, entre otras cosas). Por desgracia, son una excepción, ya que nadie más financia proyectos de código abierto, trabajos de localización y auditorías de *software* tan importantes.

Más información y documentación

Te recomendamos encarecidamente The Syllabus.

Además, puede consultar estos recursos para obtener más concienciación y / o aprendizaje sobre problemas y herramientas.

Privacidad, seguridad, protección, guías comunitarias y recursos

- «*Digital Resilience in the Time of Coronavirus*» («Adaptarse al mundo digital en tiempos de coronavirus», en español);
- «*Remote Work And Personal Safety*» («Trabajo a distancia y seguridad personal», en español);
- «*Community Resources for COVID-19*» («Recursos comunitarios para el COVID-19, en español»);
- Autoprotección digital contra la vigilancia;
- Kit de primeros auxilios digitales;
- Security Planner;
- Digital Public Square;
- Totem: Entrenamiento de seguridad digital para activistas y periodistas;
- «*Recommendations on Privacy and Data Protection in the Fight against COVID-19*» («Recomendaciones para proteger tus datos y tu privacidad durante la lucha contra el COVID-19», en español), de Access Now;
- Pirate Care Syllabus.

Algunas alternativas de *software* básicas

- Puedes empezar por aquí: Alternative App Centre del Kit de Data Detox;
- Si eres usuario de Android, prueba F-Droid en vez de Google Play;
- Échale un vistazo a las recomendaciones de Free Software Foundations si quieres pasarte del todo al software libre.

Soporte para herramientas digitales de código libre alternativas

- Open Tech Fund;
- Kuali Foundation;
- Linux Fundation;
- DIAL Digital Impact Alliance;
- Mozilla Grants;
- Prototype Fund;
- Open Source Observatory (OSOR)

Conceptos básicos sobre alojamiento en servidores propios

- «*Guide: What the heck is self-hosting*» («Guía: qué narices es el alojamiento en servidores propios», en español). (Introducción general);
- Awesome-Self Hosted;
- Una lista muy completa de las características de los proveedores de infraestructura de software, para usar cuando necesite decidir qué servicios usar en su contexto. (pdf);
- Lista de proveedores de alojamientos éticos y autónomos (pdf)

Más información sobre Zoom

Si sigues usando o promoviendo el uso de Zoom, léete estos artículos:

- «*Do you know how Zoom is using your data? Here's why you should*» («¿Sabes cómo usa Zoom tus datos? Esto te interesa», en español;
- «*Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*» («Las reuniones de Zoom no están cifradas de extremo a extremo, pese a lo que dice su *marketing*», en español)*;*
- «*Working From Home? Zoom Tells Your Boss If You're Not Paying Attention*» («¿Trabajas desde casa? Zoom avisa a tu jefe si no estás prestando atención», en español);
- «*A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*» («Una función de Zoom mostraba en secreto datos de perfiles de Linkedin», en español);
- «*'Zoom is malware': why experts worry about the video conferencing platform*» («"Zoom es un programa malicioso": por qué a los expertos les preocupa está plataforma de videoconferencias», en español);
- «*FAQ on Zoom Security Issues*» («Preguntas frecuentes sobre los problemas de seguridad de Zoom», en español).

Este artículo se publicó por primera vez en la página web de Tactical Tech

Agradecimientos: gracias a Alexander Ockenden, Christy Lange, Danja Vasiliev, Jacopo Anderlini, Laura Ranca, Manuel Beltrán, Wael Eskandar por sus comentarios, críticas, sugerencias y correcciones, y, sobre todo, muchísimas gracias a Stephanie Hankey,

---

Este artículo fue traducido del inglés al español como parte de una serie de recursos y publicaciones producidos por Exposing the Invisible durante un proyecto de un año (septiembre de 2020 - agosto de 2021) apoyado por la Comisión Europea (DG CONNECT)

European Commission

Este texto refleja la opinión de los autores y la Comisión no es responsable del uso que pueda hacerse de la información contenida en el texto.
