DERECHOS HUMANOS Y SEGURIDAD DIGITAL

CodeandoMéxico

CAPÍTULO Ø1

Ante el contexto en el que se desarrollan las actividades de las personas defensoras de derechos humanos en América Latina, su seguridad es una preocupación constante. En la práctica, existen muchos elementos que dificultan la creación y puesta en marcha de planes integrales de protección, como la falta de tiempo, recursos y/o conocimiento.

/ Considerando la seguridad desde una perspectiva holística, lo digital se integra como una dimensión más a la seguridad física y la seguridad psico-social. Comúnmente, al menos de forma intuitiva, al generar planes de protección se prioriza la seguridad física, pese a que en diferentes reportes y encuestas se ha mostrado cómo las personas defensoras de derechos humanos tienen incidentes de seguridad digital y se sienten vulnerables al usar tecnología.

/ Esto se debe a que actualmente la tecnología funciona como una caja negra en la que sólo vemos lo que ocurre al final del camino, pero desconocemos cómo se llevan a cabo los procesos y como están hechos los dispositivos que usamos, lo cual dificulta entender en dónde están las vulnerabilidades y cómo protegerse.

ACTIVIDAD
¿ALGUNA VEZ HAS HECHO UN ANÁLISIS DE RIESGO?

Existen diferentes metodologías para desarrollarlos. Ahora te proponemos una actividad muy sencilla pero poderosa para que reflexiones sobre la importancia de la seguridad digital en tu contexto*.

/ En la siguiente imagen:

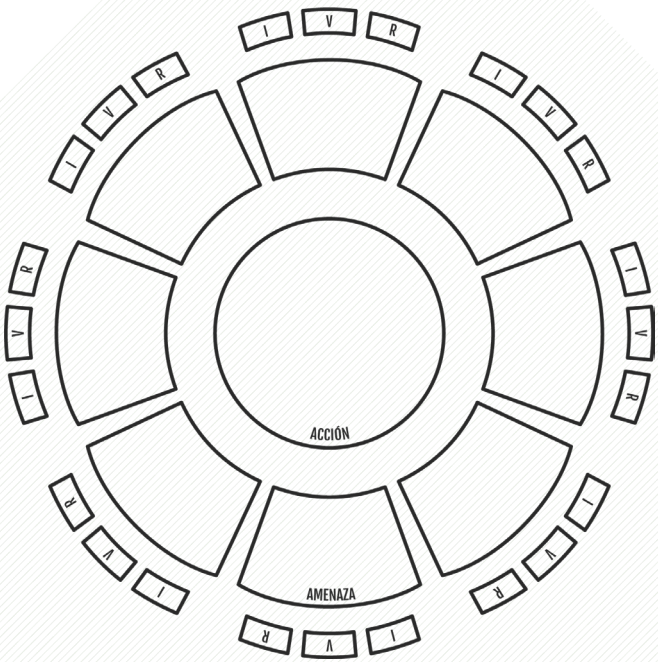
1/ **Escribe la acción sobre la cual harás tu análisis.** Ej:, "Comunicación por grupos de WhatsApp" (puede ser un grupo en específico)

2/ **Piensa en amenazas que pudieran afectar esta acción.** Ej: "Robo de celular", "Captura de pantalla por parte de algún integrante de los grupos", "Que el teléfono quede sin capacidad de almacenar información".

3/ Para los **Riesgos, Vulnerabilidades e Impactos ilumina el color que corresponde de acuerdo a tu contexto.**

DEFINICIONES:

- **Amenaza:** algo que me hace daño (considera que en algunos casos aún cuando la amenaza no se haya concretado su posibilidad de existencia puede dañar).
- **Riesgo (R):** la posibilidad de que se materialice el daño (rojo: posibilidad alta, naranja: media, verde: baja).
- **Vulnerabilidad/capacidad (V):** ¿qué tan preparada estoy para enfrentar esta amenaza? (rojo: poco preparada, naranja: medio preparada, verde: muy preparada).
- **Impacto (I):** si pasa, ¿qué tan grave sería? (rojo: gravísimo, naranja: más o menos grave, verde: no es grave).



- **Toma un momento para observar tu actividad completa**, ¿qué tan roja, amarilla o verde se ve?, ¿qué te hace sentir?, ¿hay alguna acción que puedas tomar para prevenir o contrarrestar estas amenazas?

** Esta actividad es resultado de reflexiones de mujeres latinoamericanas y sigue en construcción, puedes mejorarla y compartirla a quien la necesite.*

CAPÍTULO Ø2

En 2016, una de las organizaciones que ha dado seguimiento a casos de vigilancia y espionaje digital en contra de defensores de derechos humanos, CitizenLab publicó el reporte “El disidente del millón de dólares”, el cual documentó el uso de tres tipos de productos informáticos para interceptar comunicaciones del activista Ahmed Mansoor, ganador del premio Martin Ennals Award (conocido también como el “Premio Nobel para los derechos humanos”).

/ Mansoor, residente de los Emiratos Árabes Unidos, fue atacado con programas de las compañías Finfisher, Hacking Team y NSO Group[1]. De acuerdo con los reporte de estas compañías sus productos son vendidos de forma legal para gobiernos democráticos, fuerzas de la ley y agencias de inteligencia para combatir amenazas como crimen organizado o terroristas. Sin embargo, lo ocurrido con Mansoor revela su uso contra defensores de derechos humanos.

/ Tal vez esta historia suene geográficamente muy lejana, no obstante, existen evidencias de que la censura, la vigilancia y el espionaje en medios digitales han crecido también en la región latinoamericana. Por ejemplo, a partir de la exposición de información reservada de Hacking Team se reveló que mantuvieron negociaciones en al menos 13 países en América Latina[2] y México fue el país que más regalías dio a esta compañía al gastar 5,808,875 euros[3].

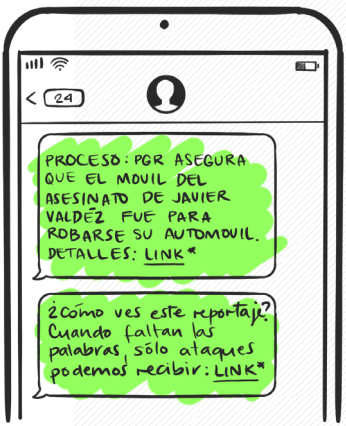
/ Hacking Team vendió a diferentes entidades gubernamentales su plataforma, conocida como *Control Remoto Galileo*, para interceptar información. En el caso de Puebla, durante el periodo del gobernador Rafael Moreno Valle, *Galileo* fue usado contra periodistas, adversarios políticos y académicos[4].

/ Desafortunadamente y pese a la exposición pública de estos casos, se han seguido adquiriendo programas para la vigilancia para ser usados contra personas defensoras de derechos humanos.

/ En la última actualización[5] (marzo, 2019) para México de la investigación del uso de *Pegasus*, el sistema vendido por NSO Group, se confirman 25 blancos entre los que se encuentran periodistas, abogados de derechos humanos, legisladores y el Grupo Interdisciplinario de Expertos Independientes (GIEI) que participó en la investigación del caso Ayotzinapa.

¿CÓMO OPERA PEGASUS?

Hasta ahora lo que se ha visto es que **el ataque inicia cuando recibes un mensaje de texto (sms) acompañado por un link**. La información que contiene el mensaje está encaminada a que tu primer impulso sea abrir el link sin reflexionarlo. Por ejemplo, en el Caso de Griselda Triana, esposa de Javier Valdéz, recibió estos dos mensajes:



*El link original se puede ver en la fuente [5]

/ El LINK aparenta ser de un sitio web legítimo, sin embargo, estás entrando a un sitio que buscará instalar un programa informático malicioso (*malware*) que iniciará un ataque para tomar el control del dispositivo. El sistema está diseñado para no dejar rastros desde dónde se hicieron estos ataques. Si se logra la infección, el atacante logrará tener acceso total al dispositivo. En el caso de teléfonos móviles podrá acceder al micrófono, cámara, mensajes de texto, escuchar llamadas telefónicas, contenido de aplicaciones, etc.

/ En México, el costo que tuvo la contratación de *Pegasus* es desconocido y existen evidencias de irregularidades en su adquisición[6].
Para darnos una idea, en 2016 el New York Times reveló que para la infección de 10 iPhones el costo es de $650,000 dólares más una membresía de $500,000 dólares[7].

/ Para conocer más puedes ver la investigación de "Gobierno espía"[8].

1 *The Million Dollar Dissident.* Bill Marczak and John Scott-Railton. https://is.gd/odqSkg
2 *Hacking Team en América Latina.* Derechos Digitales. https://is.gd/8rJ0kE
3 *Hacking Team Emails Expose Proposed Death Squad Deal, Secret U.K. Sales Push And Much More.* The Intercept. https://is.gd/bKpN8W
4 *El gobierno de Puebla usó el software de Hacking Team para espionaje político.* Animal Político. https://is.gd/utZoOB
5 *Reckless VII.* The Citizen Lab. https://is.gd/Xu4PrE
6 *Pegasus, posible negocio redondo que involucra a altos funcionarios: MCCI.* Aristegui Noticias. https://is.gd/rXN3iv
7 *How Spy Tech Firms Let Governments See Everything on a Smartphone.* The New York Times. https://is.gd/x3yp96
8 *Gobierno Espía.* ARTICLE 19 *et al.* https://is.gd/MERKvz

CAPÍTULO Ø3

El término “Seguridad Digital” no tiene una definición única y estática. Esto es porque la seguridad no es un estado absoluto, depende de varios factores, como el contexto de las personas y lo que perciben como “seguro”, de tal forma que la definición requiere una reflexión propia y colectiva. En este fanzine, nos referiremos más en sentido práctico al conjunto de herramientas y estrategias que emplearemos para protegernos al usar medios digitales, por ejemplo, teléfonos móviles o computadoras portátiles.

/ Cuando hablamos de lo digital hay cuatro aspectos que podemos tratar de proteger[9]:

UBICACIÓN

Dependiendo de la actividad que realizas y el tipo de dispositivo, la ubicación puede ser revelada por cosas como la dirección IP[10] que tienes asignada.

CONTENIDO

De nuestras comunicaciones.

INFORMACIÓN

Personal Sensible e Información Personal Identificable[11]

REDES SOCIALES Y CONTACTOS

Aquí nos referimos no a tus cuentas en redes sociales comerciales, sino a quienes efectivamente constituyen tus redes.

[9] *Instituto de Genero y Tecnologías para defensoras de la tierra en América Latina.* Alexandra Hache. *https://is.gd/dpqzxV*

[10] IP viene del inglés *Internet Protocol* y hace referencia al protocolo que se usa para la transferencia de información entre un origen y un destino. Contempla intercambio de datos en redes y sistemas interconectados. Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) y es asignada por el proveedor de servicios de telecomunicaciones. *Dirección IP*. Wikipedia. *https://is.gd/vrMuC7*

/ El dilema es que proteger implica también emplear más energía (tiempo-recursos), por lo que es necesario priorizar.

/ Las estrategias de resistencia[12] podemos dividirlas también en cuatro:

1/ REDUCIR *En algunas circunstancias menos es más.* Por ejemplo, a veces tenemos muchos correos electrónicos (el primero que tuve y le puse un nombre chistoso, el personal, el del trabajo, etc.) y muchas veces nos reenviamos correos entre ellos para respaldar. Eso va dejando rastros de nuestra información, ¡por muchos lados!	**2/ OFUSCAR** Ofuscar es *tratar de confundir a quien busque atacarnos.* Podemos crear muchos perfiles sobre uno mismo con información diversa que confunda sobre cuál es el perfil verdadero.
3/ COMPARTIMENTAR Compartimentar es *dar un lugar a cada cosa.* Por ejemplo, usar un teléfono para las actividades del trabajo y otro para las personales.	**4/ FORTIFICAR** Fortificar es *tratar de poner barreras más poderosas*, como contraseñas fuertes en todas nuestras cuentas.

Lo que hay que recordar es que no hay recetas sobre cómo tener mayor seguridad digital, depende de cada caso y es un proceso que se construye de acuerdo a las necesidades y prioridades de cada persona.

[11] La información personal sensible son los datos de una persona que si se revelan puede tener un efecto negativo, como su cuenta bancaria o sus contraseñas de correo. La Información personal identificable (PII por sus siglas en inglés) se refiere a toda aquella información sobre un individuo que es administrada por un tercero (p. ej. gobiernos o empresas) incluyendo todos aquellos datos que pueden ser distintivos del individuo o a partir de los cuales es posible rastrear su identidad y toda la información asociada o asociable al individuo (por ejemplo el número de su DNI, su dirección física, la placa de matriculación de su coche, etc). Pueden leer más en Mortazavi, M. y Salah, K. 2015. Privacy and Big Data in Privacy in a Digital Networked World. *Información Personal Sensible.* NA.

[12] *Strategies Of Resistance.* My Shadow. *https://is.gd/VnzwgX*

CAPÍTULO Ø4

Es común que las herramientas digitales que se van integrando a nuestro trabajo no han sido elecciones informadas. Tal vez inicialmente se usaron porque son de las compañías más grandes en el mercado y las que más se promocionan, porque ofrecen servicios supuestamente "gratuitos" o porque son las que venían instaladas en los dispositivos. Esto hace que las herramientas no sólo puedan ser inseguras, sino que además no sean las más eficientes.

/ Pero **¿cómo se puede hacer una elección informada de herramientas digitales?**

/ Primero **considera todos los usos, necesidades y recursos** con los que cuentas. Después, **investiga qué herramientas existen** que sean útiles para lo que tu requieres y que se encuentren dentro de lo que definiste en el primer paso. Por último, **investiga el compromiso con la privacidad y la seguridad de la herramienta** y si efectivamente lo aplican.

/ Aquí dos guías que te ayudarán:

GUÍA 01. TU HERRAMIENTA [13]

[13] Modificado de *Technology tools in human rights.* 2016. Engine Room https://is.gd/VESCq0

3. ¿En qué dispositivos?¿Qué sistemas operativos soporta?

¿Se puede instalar en teléfonos móviles y computadoras?

¿Se puede instalar en sistemas Windows, Mac o Gnu-Linux?

4. Si será usado por un equipo de trabajo, ¿se cuenta con los recursos necesarios?

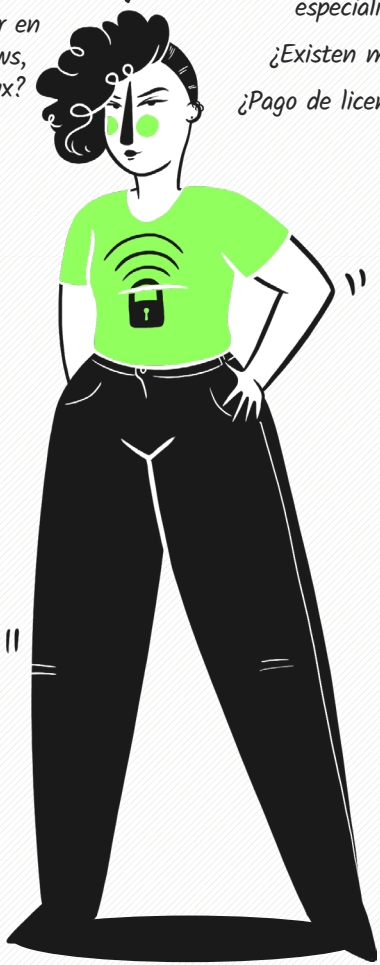
¿Idiomas necesarios?

¿Configuraciones técnicas?

¿Conocimientos especializados?

¿Existen manuales?

¿Pago de licencia de uso?



GUÍA 02. EVALÚA LA HERRAMIENTA

¿Cómo puede una persona no "especialista" evaluar una herramienta desde la seguridad y la privacidad? La mejor respuesta que hemos encontrado es: **haciendo más preguntas e investigando.**

/ Por ejemplo, iniciemos con el **dinero.** ¿Cómo se sostiene esta herramienta? Podría sostenerse por donaciones, ofreciendo servicios o *¡vendiendo tus datos!*

/ También podrías querer conocer **qué tan transparente es** la compañía/organización que mantiene la herramienta: ¿hace informes de transparencia?, cuando se han reportado fallos de seguridad, ¿da respuestas públicas?, ¿cómo son sus políticas de privacidad? ¿son claras?, cuando recibe requerimientos gubernamentales, ¿los reporta?

/ Existen también algunos **aspectos técnicos** como si la herramienta fue auditada, si usa mecanismos de cifrado[14] o si su código es libre (software libre)[15].

/ **Si quieres conocer más** revisa los materiales de Género y Tecnología[16] y la sección de documentos de Técnicas Rudas[17].

[14] En criptogafía el cifrado es el procedimiento para convertir una serie de datos o información en una cifra o código de manera que solo pueda interpretarse y ser leída por aquella persona que tenga la manera de revertir el proceso, por ejemplo, con una contraseña o una clave de cifrado. *Cifrado.* NA

[15] Software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. *Software libre.* NA.

[16] *Recursos de Género y Tecnología.* Tactical Tech. *https://is.gd/0osExy*

[17] *Recursos de Técnicas Rudas.* Técnicas Rudas. *https://is.gd/QsK0ZJ*

CAPÍTULO Ø5

Una forma eficiente para combinar la seguridad digital junto con las dinámicas de trabajo es pensar en términos de **ecosistema tecnológico**.

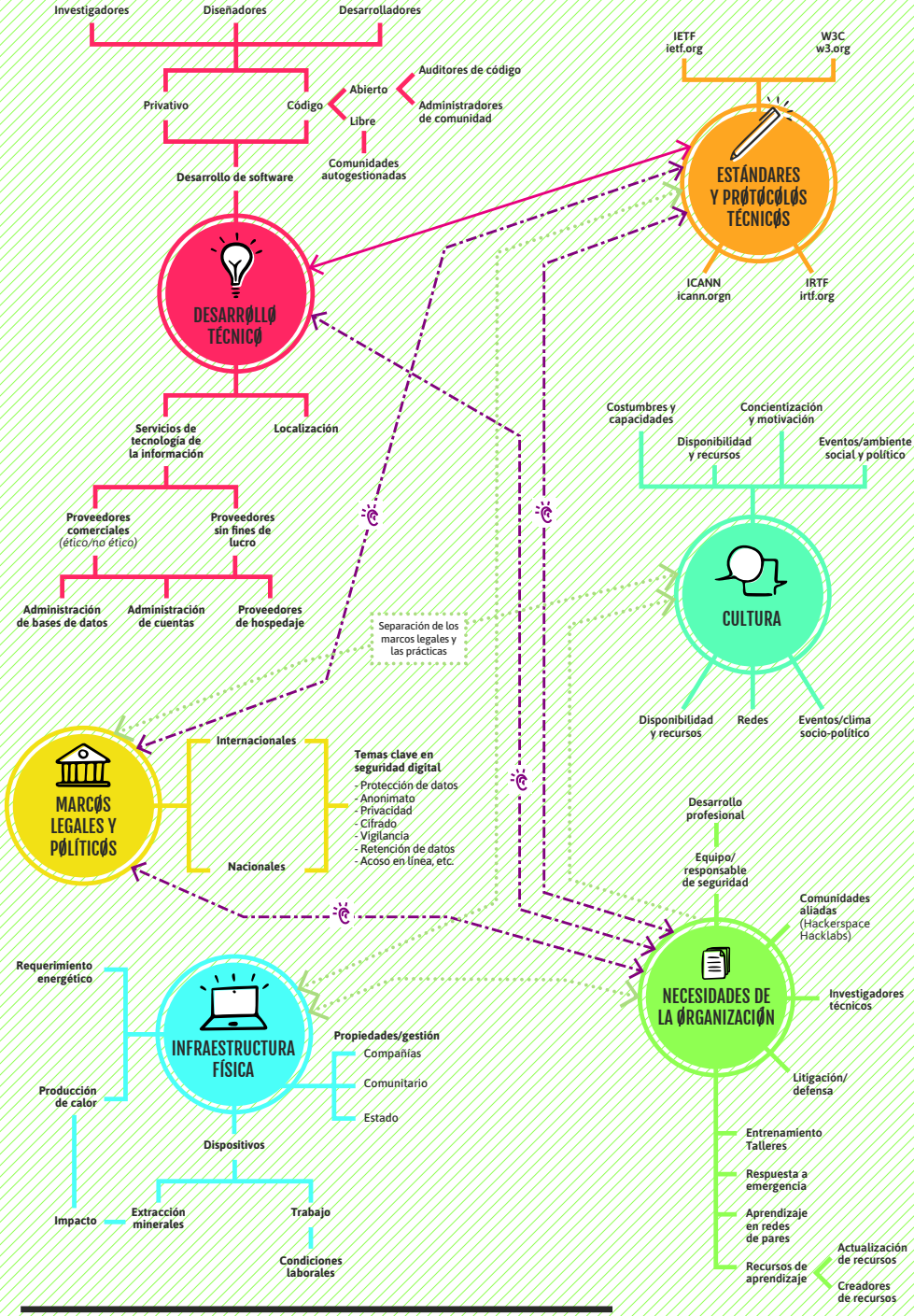
/ Lo interesante de abordarlo desde la perspectiva de los ecosistemas es que permite visualizar comunidades, sus interacciones internas y con otras comunidades, infraestructura, plataformas y programas específicos. Nos permite también integrar dimensiones menos tangibles como la dimensión política sobre la justicia social (libertad vs vigilancia y censura, obsolescencia programada, explotación de territorios y de personas vs trabajo digno y la búsqueda de la sustentabilidad en el uso de recursos), etc.

/ El proceso de usar herramientas tecnológicas (o peor aún que las herramientas tecnológicas nos usen) al estar dentro de las dimensiones de los ecosistemas tecnológicos nos ayuda a movernos hacia las tecnologías sociales, a lograr soberanía/autonomía tecnológica para los pueblos.

> *La soberanía tecnológica nos remite a la contribución que hacemos cada una de nosotras al desarrollo de tecnologías, rescatando nuestros imaginarios radicales, rescatando nuestra historia y memorias colectivas, re-situándonos para poder soñar y desear juntas la construcción aquí y ahora de nuestras infraestructuras propias de información, comunicación y expresión.*
>
> *Alexandra Haché, Soberanía Tecnológica*

ECØSISTEMA DE SEGURIDAD DIGITAL*

HAZ ZOOM IN PARA VER TODO



*Mapa adaptado de *"Ties that bind organisational security for civil society"* creado por The Engine Room

CAPÍTULO Ø6

Hasta aquí tal vez todo suena muy bien, tecnologías sociales, ecosistemas tecnológicos, estrategias y herramientas para la seguridad digital, pero al final del día **¿cómo lo integramos en nuestras vidas?**

/ Es posible que ya tengas prácticas integradas y/o que ya uses algunas de las herramientas y lo que falta puede parecer mucho, pero hay que recordarnos que todo es un proceso y puede llevar un tiempo.

/ Ahora veremos ejemplos simples para ir dando los primeros pasos:

1 / MAPAS

¿Cómo recopilamos y visualizamos información geográfica, tanto para fines de análisis interno como para la generación de mapas públicos? Por facilidad, tendemos a usar Google Maps. Google es uno de los hipergigantes de la tecnología, con ganancias cuantiosas comparables con el Producto Interno Bruto de algunos países, prácticas laborales nocivas[18], profundo impacto ambiental y explotación de usuarios/as[19] [20].

/ De forma alternativa existe **Open Street Map** (openstreetmap.com), un proyecto colaborativo de información geográfica que está pensado para ser alimentado y usado por cualquier persona. Es posible usarlo dentro de dos aplicaciones que te podrían ser útiles: OsmAnd y Umap.

/ **OsmAnd** es una aplicación de mapas y navegación para teléfonos móviles que integra datos de OpenStreetMap y de Wikipedia para que puedan ser usados incluso sin conexión a internet. Con la integración de extensiones puedes trazar tus propios puntos o rutas, tomar imágenes o vídeos georeferenciados y también alimentar la base de datos de OpenStreetMap.

[18] *Fuck off, Google!* https://is.gd/jDTsR6

[19] *¿Territorio internet? Espacios, afectividades y comunidades.* la_jes. https://is.gd/cWEwBj

[20] *How to stop data centres from gobbling up the world's electricity.* Nature. https://is.gd/nop16b

/ Con esta herramienta puedes recopilar y administrar información geográfica, así que puedes mantenerla privada o ponerla pública. Si decides ponerla pública, puedes hacerlo en OpenStreetMap directo desde la aplicación o en **Umap**[21], una fantástica herramienta para hacer mapas que estarán disponibles por internet.

2 / DOCUMENTOS

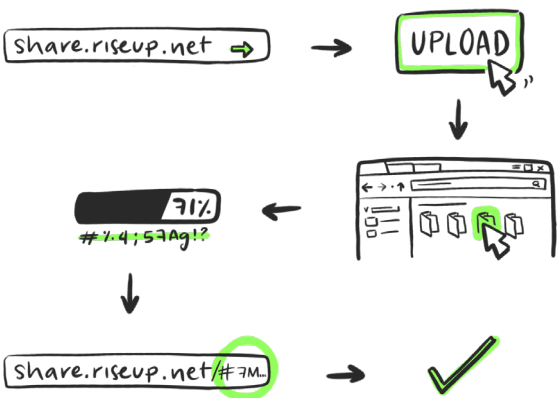
Muchas veces tenemos que compartir documentos que no podemos enviar por correo electrónico, así que es posible que recurramos a servicios comerciales (incluso si no te cobran por usarlos su modelo de negocio está basado en el lucro).

/ Una alternativa es usar **share.riseup.net**. Es bastante intuitivo:

1/ Entrarás a un sitio web con un **cuadro que dice "upload" (subir), dale click**.

2/ Se abrirá un explorador de archivos, **selecciona el archivo que quieres cargar.**

3/ Mientras se guarda, el contenido se cifra y al finalizar el link del sitio ha cambiado. **Copia el link y compártelo con quienes tú elijas.**



3 / COMUNICACIONES

Es posible que tus comunicaciones instantáneas las hagas preferentemente por WhatssApp. Esta aplicación pertenece a una compañía nefasta que está al servicio del poder, Facebook, la cual ha tenido múltiples reportes de fallos de seguridad (el más reciente fue una vulnerabilidad que permitía a un atacante hacer una llamada que no sería registrada por el usuario y que lograría inyectar código malicioso)[22].

/ Una alternativa más segura e incluso divertida es **Wire**. Wire tiene un modelo de negocio basado en ofertar servicios, tiene estándares de cifrado fuertes y su política de privacidad integra que sus servidores operen bajo las legislaciones que dan la mayor protección a sus usuarios/as.

/ Algunas funcionalidades son el poder crear grupos, hacer llamadas/video-llamadas grupales, compartir ubicación, distorsionar la voz en mensajes, desaparecer automáticamente mensajes, entre otras. Está disponible para teléfonos y computadoras de escritorio y para diferentes sistemas operativos.

Estos son sólo tres ejemplos de herramientas útiles **pero antes de usarlas** hay dos preguntas fundamentales que te puedes hacer:

1/ ¿Cómo integrarías estas herramientas dentro de tu flujo de trabajo?

2/ ¿Cómo podrían formar parte de tu estrategia de seguridad?

[21] Por ejemplo *https://umap.openstreetmap.co/es/* uMap. *uMap*

[22] *WhatsApp voice calls used to inject Israeli spyware on phones.* Financial Times. *https://is.gd/MZhtCP*

CodeandoMéxico

Redacción
Anamhoo

Edición y revisión
Codeando México

Diseño editorial e ilustraciones
Citlalli Dunne

Este fanzine fue realizado gracias al apoyo de:

Australian Aid