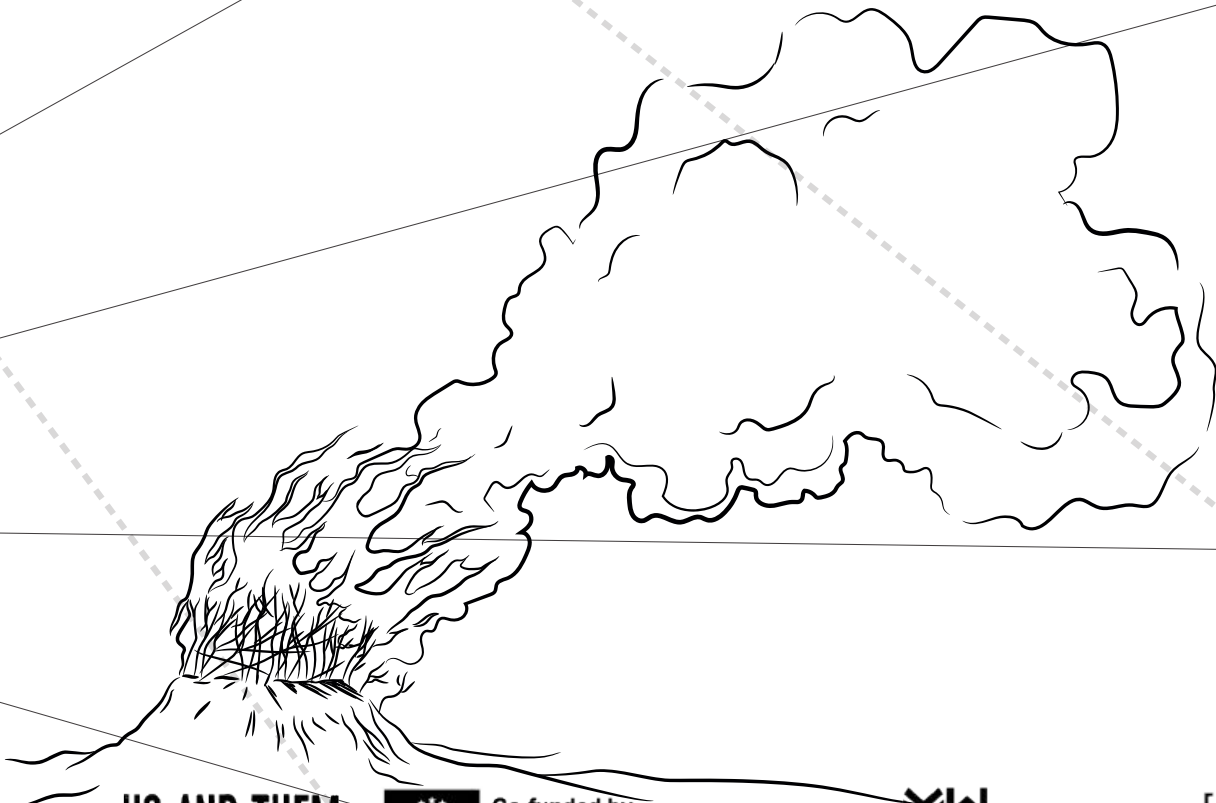




& / AUTODEFENSA  
DIGITAL



US AND THEM



Co-funded by  
the European Union

MW  
maghweb

*crisis*

[EdIPo]  
Equipo de Investigación Política

~~SEGURIDAD~~ CUIDADOS  
~~ESTADO~~ PROCESO  
~~INDIVIDUAL~~ COLECTIVO

## UNA INVITACIÓN A PENSAR VÍNCULOS y HÁBITOS

¿cómo son los territorios por donde transitamos y nos relacionamos?

¿en qué condiciones los habitamos?

¿qué rastros dejamos al atravesarlos?

ejercitar una reflexión activa sobre nuestras prácticas cotidianas en el entorno digital, explorar nuevos hábitos de atención y cuidado (de nuestros datos y de quienes nos rodean) e implementar políticas de reducción de daños lleva tiempo (paciencia) y trabajo, pero no de forma solitaria: se construye con otrxs en un proceso abierto de aprendizaje continuo. su sustentabilidad depende de que sea un recorrido colectivo y situado, construyendo estrategias a partir de nuestra realidad.

si la impotencia paraliza compartir las preguntas y el conocimiento sobre las herramientas que usamos junto con sus alternativas nos devuelve la agencia para ampliar nuestros márgenes de acción y autonomía.

invitamos a lo que funciona  
en cada contexto ritmo

si la cantidad de información abruma  
toma lo ue sirva y circula lo demás

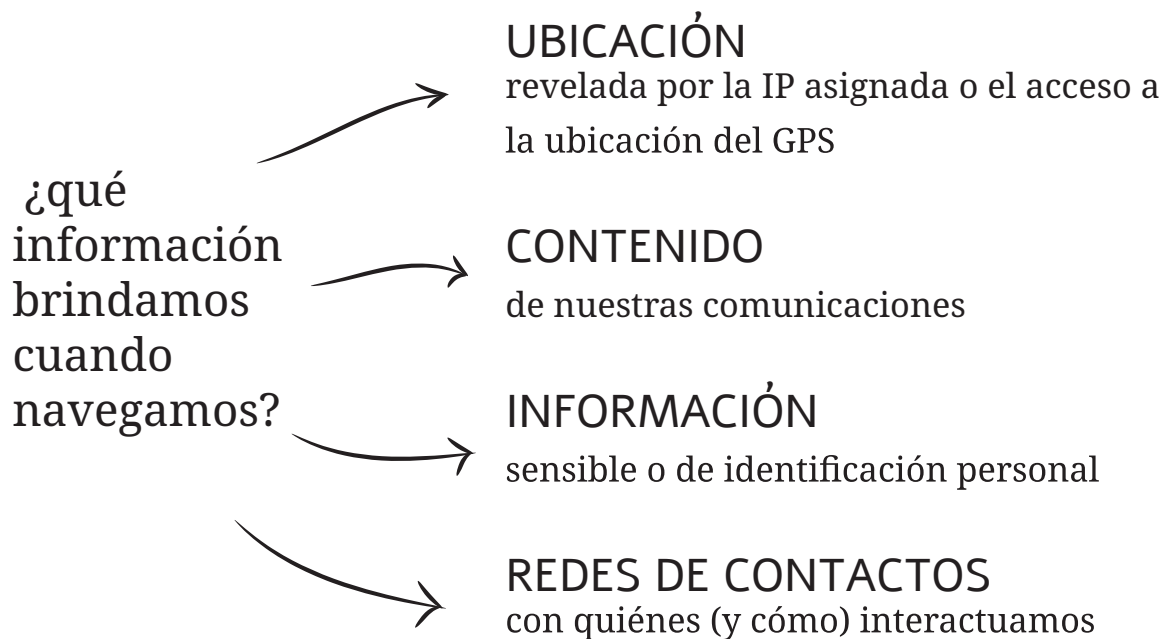
# ESTRATEGIAS DE RESISTENCIA

REDUCIR\_ ANDAR LIGERX (DEJAR MENOS RASTROS ¿QUÉ DATOS BRINDAMOS? ¿HASTA DÓNDE Y CÓMO NECESITAMOS IDENTIFICARNOS?)

OFUSCAR\_ CONFUSIÓN MULTIPLICIDAD DIFUSIÓN DE IDENTIDADES

COMPARTIMENTAR\_ CADA COSA EN SU LUGAR /SEPARAR PERFILES

FORTIFICAR\_ FORTALECER LAS BARRERAS QUE PROTEGEN NUESTRA INFORMACIÓN



# MODELO PARA (DES)ARMAR

## EJEMPLO DE ACTIVOS

canales de comunicación del colectivo  
datos personales de lxs miembrxs  
datos de la comunidad que nxs sigue o participa de los eventos

Para diseñar estrategias de cuidado colectivo

necesitamos identificar primero qué nos interesa proteger (activos) frente a qué o quién (adversarios).

¿alguien conocido como una expareja?  
¿un anónimo de internet?  
¿el gobierno?  
¿empresas de publicidad?

¿con qué recursos económico, sociales, técnicos cuenta para acceder a ellas?

¿con qué recursos o herramientas contamos nosotrxs?

Una lectura de capacidades/vulnerabilidades nos ayuda a percibir la probabilidad (posibilidad de que ocurra) y el impacto (gravedad de las consecuencias) de cada amenaza concreta.

Definirlas con precisión permite orientar acciones de mitigación y planificar en función de los recursos disponibles.

algo que me hace o puede hacer daño

A CONTINUACIÓN UN MAPA CON HERRAMIENTAS ALIADAS PARA LA MITIGACIÓN DE RIESGOS EN CONECTOS ACTIVISTAS





# protondrive

Servicio de almacenamiento en línea encriptado con un máximo de 1GB por cuenta

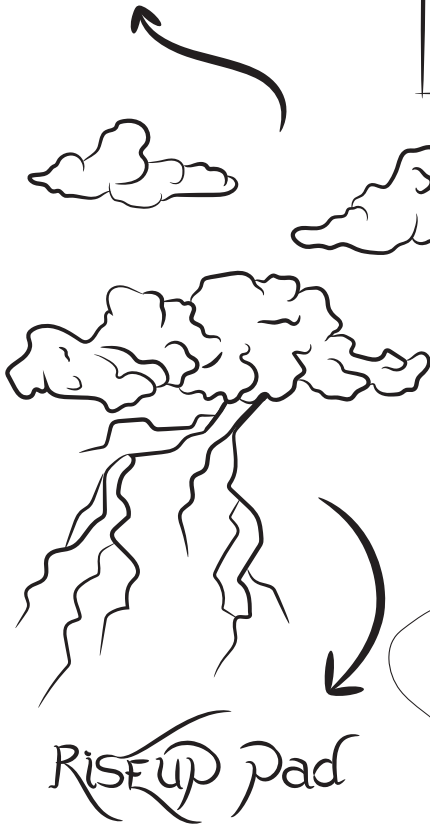
# cryptpad

Espacio de colaboración en línea que permite trabajar hojas de calculo, documentos de texto, kanban, formularios y diapositivas  
Ofrece servicio de almacenamiento en línea encriptado con un máximo de 1GB

No son una solución mágica  
-ni de

✓ código abierto

✓ versión gratuita



# RiseUp Pad

Permite crear documentos colaborativos en línea con posibilidad de programar su autodestrucción



# VERACRYPT

Herramienta para el cifrado de discos y carpetas en la PC/pendrives

# KEEPASS

Herramienta para la gestión segura de contraseñas diversas mediante una única "llave maestra"



# Wormhole

Permite compartir mediante enlaces de caducación automática archivos de hasta 10GB cifrando el contenido de extremo a extremo

Ninguna herramienta sirve si no está actualizada

finitiva  
to

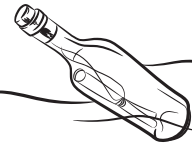
# HERRAMIENTAS

para la

# Aula Defensa

Tails

Sistema operativo paralelo portátil de naturaleza anónima y amnésica. Ofrece una selección de herramientas para el trabajo con información sensible y la comunicación segura



Protonmail

Correo electrónico cifrado de extremo a extremo

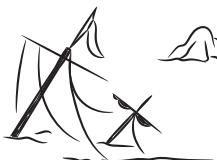
Tor

Cifra tres veces el tráfico de datos y los redirige a través de servidores aleatorios de esta red para ocultar su origen y destino

Bloquea rastreos y accesos al contenido de tu navegación a terceros

VPN

anonimiza la locación y  
cripta el tráfico de datos  
(recomendamos Riseup VPN)



## NAVEGACIÓN

1- VPN: <https://riseup.net/en/vpn>

anonimiza la locación y encripta el tráfico de datos. esquivas censuras y evita rastreos con fines de vigilancia o publicidad.

¿cómo? una conexión encriptada canaliza a través de sus servidores seguros tu tráfico hacia el internet público como si fuese un túnel.

recomendamos RISE UP VPN porque además de ser gratuita no registra dirección IP (pero debe ser activada cada vez)

+ también disponible para ANDROID

(alternativas ProtonVPN, NordVPN, Tunnel Bear)

2- TOR: <https://www.torproject.org/es/download/>

cifra tres veces el tráfico de datos y lo redirige a través de servidores aleatorios de la red tor para ocultar su origen y destino. bloquea rastreadores e invisibiliza el contenido de tu navegación a terceros

Tor cifra y anonimiza tu conexión al pasarlo a través de 3 relays. Los relays son servidores operados por diferentes personas y organizaciones de todo el mundo. Tor evita que alguien que esté viendo tu conexión a Internet sepa qué estás haciendo en Internet.

## COLABORACIÓN

3- WORMHOLE: <https://wormhole.app/>

Cifrado de extremo a extremo y enlace de caducación automática para el envío de archivos de hasta 10 GB. Solo se mantiene en la nube max 24hs y se autodestruye.

4- CRYPTPAD: <https://cryptpad.fr/>

Espacio de colaboración y almacenamiento en línea encriptado de extremo a extremo con posibilidad de trabajar hojas de cálculo, documentos de texto, kanban, códigos, formularios, pizarras y diapositivas con un max. de 1 GB. OJO! si olvidas la contraseña no es posible recuperarla.

5. PAD RISE UP: <https://pad.riseup.net/>

Permite crear de forma sencilla documentos colaborativos alojados en servers seguros con posibilidad de programar su autodestrucción. Además, funciona como alternativa para chatear sin necesidad de compartir aplicación.



## RESGUARDO DE INFORMACIÓN

6- KeePass: <https://keepassxc.org/>

Gestor seguro para proteger todas tus contraseñas sin tener que recordarlas mediante una única “llave maestra”. Fabrica contraseñas seguras.

7- VERACRYPT: <https://www.veracrypt.fr/>

Cifra tus discos y carpetas “en descanso” para evitar la intromisión de terceros.

8- PROTONDRIVE: <https://proton.me/es/drive>

1 GB de espacio de almacenamiento cifrado en línea en la nube.

## COMUNICACIÓN

9- PROTONMAIL: <https://proton.me/es/mail>

Correo electrónico cifrado de extremo a extremo

10- JITSI MEET: <https://meet.jit.si/>

Software gratuito para videoconferencias sin límite de tiempo, de código abierto y con cifrado de extremo a servidor/tránsito (cifrado del dispositivo al servidor donde se descifra y se vuelve a cifrar para enviar a destino). No requiere registrarse.

11- CORREOS ELECTRÓNICOS DESCARTABLES: <https://temp-mail.org/es/> y <https://www.guerrillamail.com/es/> Direcciones de email temporales para ocultar identidad sin necesidad de registrarse.

## BÚSQUEDA DE INFORMACIÓN

12- DUCKDUCK GO: <https://duckduckgo.com/>

Motor de búsqueda que no registra datos de navegación ni orienta comercialmente los resultados en función del perfil asignado al usuario

+ Kit de ayuda para emergencias digitales

(hackeos, pérdida de información o acceso a cuentas, funcionamiento sospechosos, etc): <https://digitalfirstaid.org/es/>

# TAILS

sistema operativo portátil diseñado contra la  
vigilancia y la censura  
de naturaleza anónima y amnésica

independiente: vive en un pendrive y se  
puede utilizar desde cualquier computadora  
introduciéndolo con el dispositivo apagado

<https://tails.boum.org/>

- ✓ no deja rastros en la computadora
- ✓ software libre
- ✓ ofrece una selección de aplicaciones  
para trabajar en documentos  
confidenciales y comunicarse de forma segura:

1/2 hora  
pendrive (min 8gb)

INSTALACIÓN

- Tor Browser con uBlock, un navegador seguro con un ad-blocker
- Thunderbird, para correos cifrados
- KeePassXC, para crear y almacenar contraseñas seguras
- LibreOffice, una suite de oficina
- OnionShare, para compartir archivos a través de la red Tor
- Limpiador de metadatos.

*todo listo para usar con una configuración segura por defecto*

*y para evitar errores:*

- las aplicaciones son bloqueadas  
automáticamente si intentan conectarse  
a Internet sin Tor.
- todo en el Almacenamiento Persistente  
se cifra automáticamente.
- Tails no escribe nada en el disco duro:  
toda la memoria se borra al apagar.

MÁXIMA SEGURIDAD

GRATIS

como nadie debería pagar  
por protección en internet se  
puede copiar y distribuir de  
forma gratuita

# recomendaciones

Controlar accesos y contraseñas compartidas con google y otras aplicaciones: ¿quién tiene acceso a mis llaves? ¿a mi ubicación, mis fotos, mis conexiones y contactos?


Cambiar contraseñas viejas o repetidas e incorporar factores de autenticación. Utilizar un gestor de contraseñas externo.

Limpiar identidad virtual. Eliminar cuentas y aplicaciones fuera de uso así como todas las fotos, mensajes y correos que ya caducaron su función.


Interrumpir la emisión de señales (bluetooth, wifi, gps) y cubrir cámaras cuando no las necesitamos. Alejar el teléfono para evitar intromisiones en contextos sensibles.

Acceder a páginas solo a través de conexiones seguras (con HTTPS). Se puede configurar por defecto en cualquier navegador.

Desconfiar de los enlaces que recibimos incluso cuando conocemos el remitente. Consultar antes de abrir.



CONTRASEÑAS SEGURAS  
larga (mejor una frase)  
sin datos personales  
cambiada seguido  
no reutilizada ni con variación  
++ doble factor de autenticación  
*¿cuán segura es mi contraseña?*



<https://www.security.org/how-secure-is-my-password/>

¿cómo saber si fui  
hackeado o filtraron  
mis datos?

<https://haveibeenpwned.com/>

**US AND THEM**



***crisis***

**[EdIPo]**

Equipo de Investigación Política

