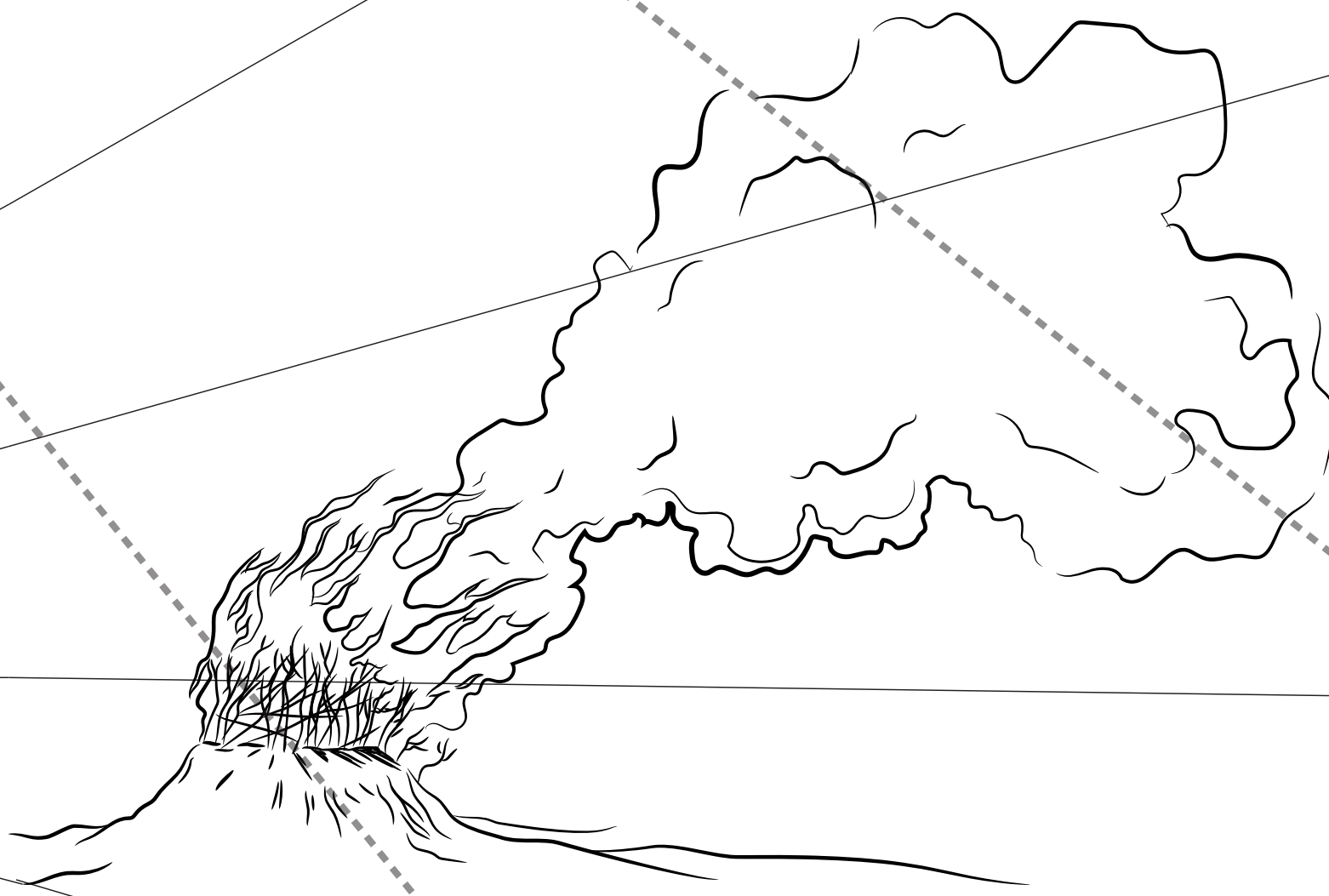
MANUAL DE CUIDADO COLECTIVO

& / AUTODEFENSA DIGITAL



invitamos a incorporar lo que funciona para cada contexto y ritmo
si la cantidad de información abruma tomá lo que sirva y circulá lo demás

UNA INVITACIÓN A PENSAR VÍNCULOS Y HÁBITOS

¿cómo son los territorios donde transitamos y nos relacionamos?

¿qué rastros dejamos al atravesarlos?

no hay recetas mágicas.
ejercitar una reflexión activa sobre nuestras prácticas cotidianas en el entorno virtual, entrenar una mirada atenta alerta abierta desde el mutuo cuidado para construir nuevos hábitos, planificar e implementar acciones preventivas

lleva tiempo y ocupa espacio

pero no es un camino solitario
sino un proceso compartido de aprendizaje continuo:
su sustentabilidad depende de que sea un recorrido colectivo y situado

si la impotencia paraliza abrir preguntas, interpelar costumbres, intercambiar experiencias en la búsqueda de herramientas nos permite ampliar

~~SEGURIDAD~~ CUIDADOS

~~ESTADO~~ PROCESO

~~INDIVIDUAL~~ COLECTIVO

No es soslayable el modelo de negocios que opera detrás de nuestras interacciones cotidianas. Nos encontramos en un ecosistema data-extractivista, gobernado por un puñado de mega empresas donde la información es sometida a un régimen de valorización, especulación y manipulación.

ESTRATEGIAS DE RESISTENCIA

REDUCIR_ANDAR LIGERX/ DISMINUIR RASTROS E IDENTIFICACIONES

OFUSCAR_CONFUSIÓN MULTIPLICIDAD DIFUSIÓN DE IDENTIDADES

COMPARTIMENTAR_CADA COSA EN SU LUGAR/ SEPARAR PERFILES

FORTIFICAR_ FORTALECER LAS BARRERAS DE PROTECCIÓN

PRIMERA LINEA DE DEFENSA

No hay herramientas tecnológicas que reemplacen practicas analógicas: *NO COMPARTIR DE MÁS*. Solo brindar la información personal o sensible absolutamente necesaria y cuando sea posible usar diversas cuentas o datos

¿QUÉ INFORMACIÓN BRINDAMOS CUANDO NAVEGAMOS?

UBICACIÓN
revelada por la IP asignada o el acceso a la ubicación del GPS

CONTENIDO
de nuestras comunicaciones

INFORMACIÓN
sensible o de identificación personal

REDES DE CONTACTOS
con quiénes y cómo intereactuamos

MODELO PARA (DES)ARMAR

una pausa a la vorágine para pensar en conjunto donde estamos paradxs

PREGUNTAS GUÍA PARA UNA EVALUACIÓN DE RIESGOS

Ejemplos
canales de comunicación del colectivo; datos personales de lxs miembrxs; datos de la comunidad que nos siguen redes o asiste a eventos.

¿**QUÉ** queremos proteger?

¿Qué ***AMENAZAS*** enfrenta?

Ejemplos
captura de contraseñas mediante phishing; acoso y acoso coordinado; acceso no autorizado a dispositivos; robo de identidad en redes sociales; monitoreo o vigilancia del gobierno; intercepción de comunicaciones

Ejemplos
una expareja; ataques aleatorios generalizados; el gobierno; empresas de publicidad; servidores de internet que conservan todos los datos de circulación no encriptados

¿De **dónde** vienen?

¿Qué tan probable es que ocurran
y qué tan grave es si sucede?

¿Con qué recursos contamos
para defendernos?

No se trata de abarcar todo sino desarrollar prácticas conscientes y posibles de reducción de daños en función de nuestros riesgos, capacidades, necesidades y prioridades.

Identificar amenazas, ordenarlas en función de su probabilidad e impacto permite orientar más eficientemente las acciones de mitigación y planificar a partir de los recursos disponibles

AMENAZA	PROBABILIDAD 1-muy baja 5-muy alta	IMPACTO 1:poco grave 5:muy grave	MITIGACIÓN ¿qué podemos hacer?	DESAFÍOS O RESTRICCIONES
Hackeo de claves mediante *phishing* -forma de engaño virtual a través de enlaces falsos-	*3*	*5*	*Incorporar factores de autenticación; utilizar un gestor de contraseñas externo; estar atentxs a los enlaces*	*Tiempo y disponibilidad para fortalecer la seguridad de claves y accesos*

Herramientas para la Auto Defensa

No son una solución mágica
-ni definitiva

✓código abierto ✓versión gratuita

ProtonDrive

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

CryptPad

4 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

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.

Riseup Pad

5 Permite crear documentos en línea colaborativos, con posibilidad de introducir contraseñas para suprotección, y programar su autodestrucción

ProtonMail

9 Correo electrónico cifrado de extremo a extremo

Wormhole

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

VeraCrypt

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

KeePass

6 Herramienta para la gestión segura de contraseñas diversas mediante una única “llave maestra”

V.P.N.

1 Anonimiza la locación y encripta el tráfico de datos (recomendamos Riseup VPN)

Tor

2 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

Ninguna herramienta sirve
si no está actualizada

Ninguna herramienta es infalible ni garantiza el 100% de anonimato en internet, pero cada una aporta diversas capas de protección. Las herramientas, al igual que los riesgos son dinámicos y exigen mantenerse informadx. Recomendamos actualizar periódicamente sistemas operativos, programas, evaluaciones y estrategias.

NAVEGACIÓN

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

anonimiza la locación y encripta el tráfico de datos. esquiva 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.

Se han detectado vulnerabilidades en algunos de sus nodos de salida, por lo que se recomienda agregar una capa extra de protección combinando su uso con una VPN.

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.

COMUNICACIÓN

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

Posee 1 GB de espacio de almacenamiento cifrado en linea en la nube.

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, 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.

El cuidado no depende solo de las herramientas: el eslabón más débil suele estar en las prácticas del usuario antes que en los dispositivos. Aunque usemos las herramientas más sofisticadas, la fuga de información es siempre una posibilidad.

Tails

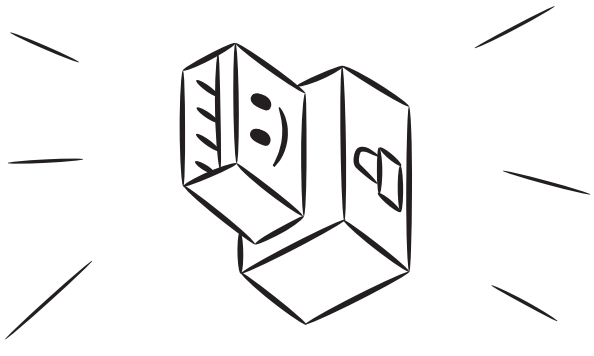
Es un sistema operativo portátil que te protege de la vigilancia y la censura

Es independiente, vive en un pendrive y se puede utilizar desde cualquier computadora

✓ **EVITA EL RASTREO**

✓ **CÓDIGO DE SOFTWARE PÚBLICO**

✓ **MÁXIMA SEGURIDAD GRATIS**



No deja rastro en la compuradora

Inicia en tu memoria USB con Tails.

Almacenamiento persistente

Puedes guardar archivos en un almacenamiento persistente

Amnésia

Todo desaparece automáticamente al apagar Tails.

Caja de herramientas

Ofrece aplicacones para trabaja en documentos sensibles y comunicarse de forma segrura

- 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 sobre Tor
- Limpiador de metadatos

https://tails.boum.org

TODO LISTO PARA NAVEGAR CON UNA CONFIGURACIÓN SEGURA POR DEFECTO

Para evitar errores:

- *Las aplicaciones son bloqueadas automáticamente si intentan conectarse a internet sin Tor.*
- *Todo el almacenamiento Persistente se cifra automáticamente.*
- *Tails no escribe nada en el disco duro. Toda la memoria se borra al apagar.*

recomendaciones

- Controlar accesos y contraseñas compartidas con Google y otras aplicaciones: ¿quién tiene acceso a mis llaves? ¿A mis ubicaciones, fotos, conexiones y contactos?

- 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.

- Desconfiar de los enlaces inesperados, incluso cuando conocemos el remitente. Chequear antes de abrir.

- Cuando sea posible optar por la eliminación automática de mensajes y por canales de comunicación que encripten la información en tráfico (de extremo a extremo).

- Cambiar contraseñas viejas o repetidas e incorporar factores de autentificación.

Es importante tener en cuenta que todo lo subido a internet permanece almacenado aunque el usuario lo borre y se oculte. Es deseable hacer una limpieza para disminuir riesgos en caso de hackeos personales, pero saber que la información no desaparece.

CRITERIOS PARA CONTRASEÑAS SEGURAS

- Larga (mejor una frase)
- Sin datos personales
- Cambiarla seguido
- No reutilizada ni con variación
- Doble factor de autenticación

IDEAL

Hacerse amigx de un gestor de contraseñas que las genere automáticamente, exija rotarlas y almacene encriptadas fuera del navegador.

¿qué tan segura es mi contraseña?

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

¿cómo saber si fui hackeadx o filtraron mis datos?

https://haveibeenpwned.com