# Introducción a la privacidad

## Y alternativas europeas


*Giorgio Mansioni*
*Enero 2026*

# ¿De qué va?

El objetivo de esta charla es concienciar sobre la importancia de la cantidad de datos que generamos y quien tiene acceso a ellos.

Además de divulgar alternativas de servicios digitales que valoren la privacidad, haciendo hincapié en el uso de tecnologías europeas, para reducir la dependencia de los ciudadanos de los servicios digitales de fuera de la unión europea.

Es un compendio de buenas prácticas y alternativas, basado en experiencias propias y aprendizajes. No una lista exhaustiva de cosas que están bien o mal.

# El precio justo

Cuando algo es gratis, el producto son **tus datos.** La mayoría de los productos “gratuitos” (navegadores, buscadores, correo, IA, ...) tienen como **modelo de negocio** venderlos directamente o perfilar y segmentar para publicidad.

Los ingresos por usuario de una empresa como Facebook (Meta) son más de 20 dólares en Europa ¿Cuantos pagáis por Instagram?
[https://www.statista.com/statistics/251328/facebooks-average-revenue-per-user-by-region/]

Las IA se nutren de nuestros datos y consultas, sin tener en cuenta regulaciones.
[https://www.abc.es/tecnologia/alemania-pide-apple-google-eliminen-aplicacion-china-20250627124540-nt.html]
Si consultas en enlace anterior compartes tus datos de navegación con 729 socios.

Wordcoint te dá 30 en euros en criptomonedas por tus datos biométricos. ¿Dinero gratis? [https://cadenaser.com/euskadi/2024/01/15/venderias-tus-datos-biometricos-te-los-compran-por-algo-mas-de-30-euros-en-bilbao-radio-bilbao/]
Aquí sólo comparten con 526 socios.

Neon la aplicación que te paga por llamar (y luego vender tus conversaciones)
[https://www.elconfidencial.com/tecnologia/2025-09-26/neon-app-pago-grabar-vender-llamadas-1qrt_4216718/]

Netflix gana más dinero con las cuentas con publicidad que con las de sin anuncios.
Temu, productos ilegales a cambio de tus datos.

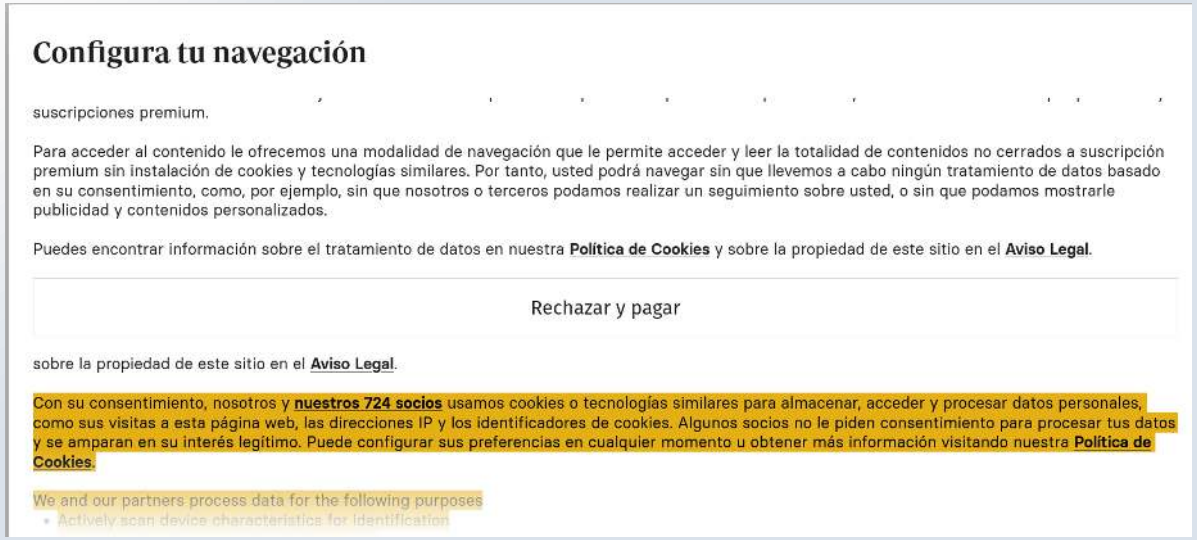
La primera buena práctica es **leer** la política de uso o los acuerdos de licencias de las aplicaciones, servicios, páginas ...

# El precio justo

Las cookies ...

Con su consentimiento, nosotros y nuestros 724 socios usamos cookies o tecnologías similares para almacenar, acceder y procesar datos personales, como sus visitas a esta página web, las direcciones IP y los identificadores de cookies. Algunos socios no le piden consentimiento para procesar tus datos y se amparan en su interés legítimo. Puede configurar sus preferencias en cualquier momento u obtener más información visitando nuestra Política de Cookies.
We and our partners process data for the following purposes

- Actively scan device characteristics for identification
- Create profiles for personalised advertising
- Create profiles to personalise content
- Develop and improve services
- Measure advertising performance
- Measure content performance
- Store and/or access information on a device
- Understand audiences through statistics or combinations of data from different sources
- Use limited data to select advertising
- Use limited data to select content
- Use precise geolocation data
- Use profiles to select personalised advertising
- Use profiles to select personalised content



# ¿Quién controla a quién?

**Europa esta llena de normativas** que parecen no tener sentido, pero algunas como la GDPR nos protege del negocio de los datos que hay en otros lugares. [https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html]

- ¿Qué pasa con mis datos si una empresa no es europea?
- ¿A quien reclamo?
- ¿Tienen obligación de borrarlos?
- Una empresa que cumple la GDPR, ¿puede transferir datos fuera de Europa?


A además, hay empresas que reconocen que si su gobierno lo pide, ellos les darán los datos de los europeos, haya acuerdo o no.
[https://www.actuia.com/es/news/datos-sensibles-y-cloud-act-microsoft-francia-admite-no-poder-oponerse-a-una-orden-estadounidense/ ]

Y a otros (supuestamente) los pillan con las manos en la masa:
[https://www.dataprotection.ie/en/news-media/press-releases/dpc-announces-inquiry-tiktok-technology-limiteds-transfers-eea-users-personal-data-servers-located]

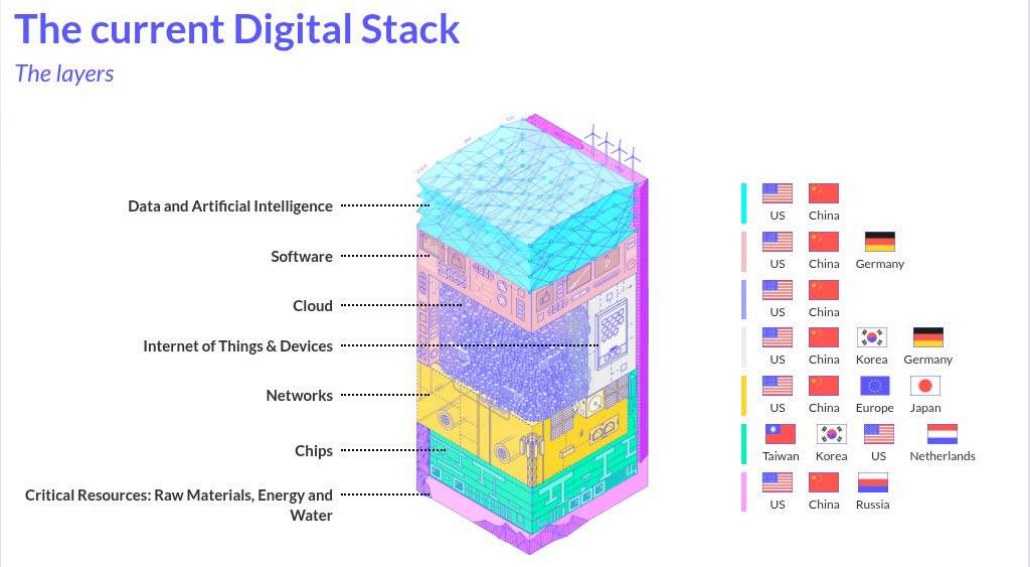
Como dice el dicho: **si no quieres que algo se sepa, no lo cuentes** (o no lo subas a Internet).

# ¿Quién controla a quién?

En la **situación geopolítica** actual, tenemos que ser conscientes de las dependencias tecnológicas de Europa, y nosotros mismos, de servicios que sobre los que **no tenemos ningún control**.

La soberanía digital en Europa no existe. A día de hoy, sólo hay planteamientos de como conseguirla. [https://www.euro-stack.info/docs/EuroStack_2025.pdf]

Ahora más que nunca, es importante el uso de software libre:
- “Because Yes”
- Porque está auditado por la comunidad.
- Libre no es gratis, los servicios tienen costes, pero no vendes tu privacidad.



# ¿Qué hay de lo mio?

Modelo de Amenazas Vs Postura de seguridad.

Tenemos que identificar las amenazas sobre nuestra información, evaluar los riesgos y las consecuencias que puedan tener.

- ¿Quien soy yo? ¿Que me preocupa?
- ¿Que pasa si me roban mis accesos? ¿Y si hay una brecha en un servicio?
- ¿Cuáles son mis amenazas a nivel de privacidad? ¿Alguien me espía? ¿Me acosa?
- ¿Qué riesgos tiene que mis datos estén "por ahí"? ¿Qué pasa si alguien sabe mi vida? ¿Me pueden perfilar para una estafa?

No es lo mismo ser un periodista en un régimen totalitario, que simplemente te preocupe que pasa con tus datos o su exposición. Hay que buscar un equilibrio respecto a nuestra situación, valorando amenazas y riesgos: No hay que volverse paranoico.

# ¿Qué hay de lo mio?

- Reducir nuestra huella y exposición digital
  - Revisar configuraciones de visualización (cuentas privadas, sólo amigos, ...)
  - Reducir uso de aplicaciones
  - Cerrar cuentas que no usemos

- Tomar consciencia de que datos compartimos
  - Leer las condiciones de uso
  - Limitar el acceso a la agenda
  - Decidir si realmente vale la pena
  - Revisar a que datos acceden las aplicaciones

- Utilizar servicios alternativos que cumplan que prioricen la protección de los usuarios y cumplan con la normativa europea de protección de datos
  - Donde se alojan los datos y quien puede tener acceso
  - Valorar los modelos de negocio de los servicios

# En su casa o en la mía

**Auto alojamiento:**
Montar un servidor propio y con software libre.

Privado porque controlas todo el proceso

✘ Conocimientos técnicos de todos los servicios, administración, backup, etc.

**Servicios de terceros:**
Buscar servicios que prioricen privacidad, no porque sean gratis.

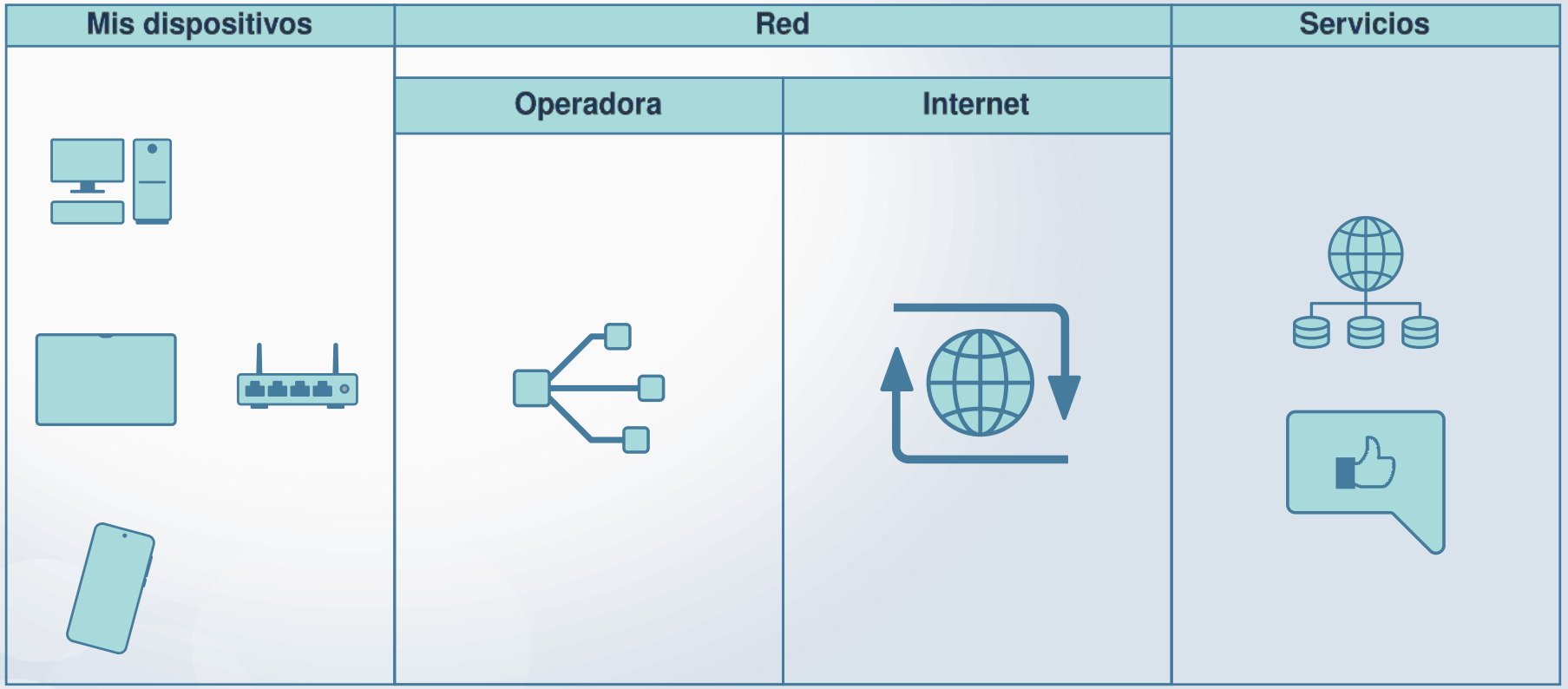
No tienes que saber de sistemas, backups, ...

✘ Requiere investigar, probar, configurar, adaptarse y hacer algún sacrificio de usabilidad.

Hablamos de ...

Telemetría, DNS seguros, VPN, Securizar el Navegador, Gestores de contraseñas, Correo electrónico y Alias, Redes Sociales Alternativas, IA Responsables, Redes descentralizadas, Metadatos, Apps alternativas en móviles, Egosurfing, ...

# Donde ocurre la magia




Simplificación de donde esta nuestra información y como tenemos que pensar a la hora de protegerla.

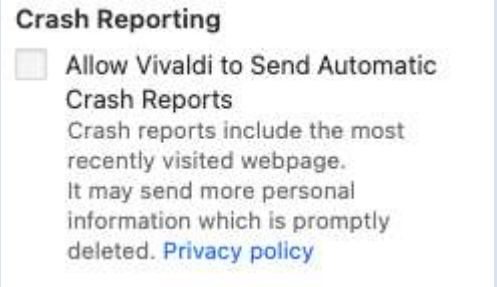
# Revisar Telemetría

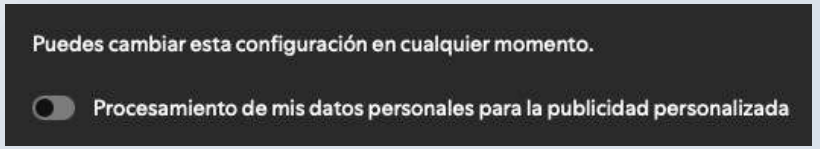
Revisar la telemetría del sistema operativo y/o aplicaciones

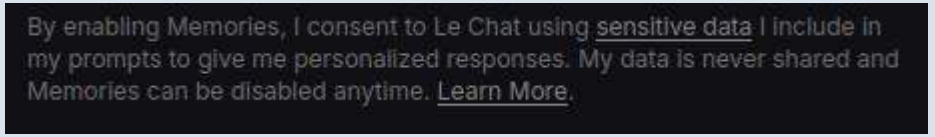
- Linux en la aplicación de configuración
- Windows y Mac necesitarás scripts.
  - https://privacy.sexy
  - https://github.com/ChrisTitusTech/winutil

Revisa las opciones de tus aplicaciones (App, Flatpak, ...)

- Opciones de privacidad, localización, segundo plano
- Perfil de usuario
- Uso de tus datos
- Rechazar cookies



# DNS

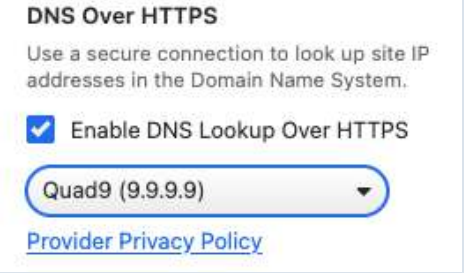
Todas las peticiones DNS que hagan nuestros equipos, pueden quedar registradas en el servidor y analizadas por el hardware intermedio que hubiera. Es una manera fácil de perfilarnos.

✘Dejar de usar los DNS por defecto de la operadora.
✘No usar los de Google (8.8.8.8) o Cloudflare(1.1.1.1).

Servicios Europeos:

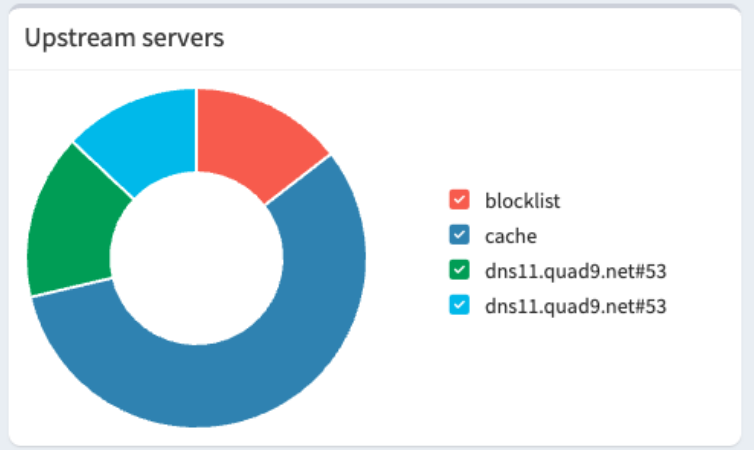
- Quad9 https://quad9.net/es/service/service-addresses-and-features/
- DNS4EU https://www.joindns4.eu/for-public

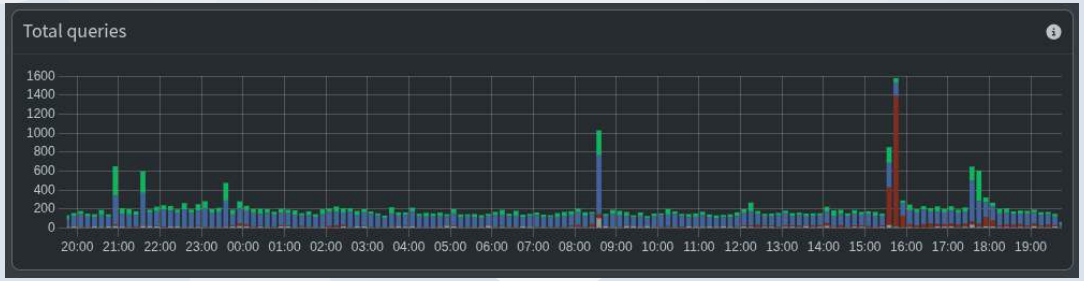
Configurar DNSSEC en los navegadores y aplicaciones que lo permitan.

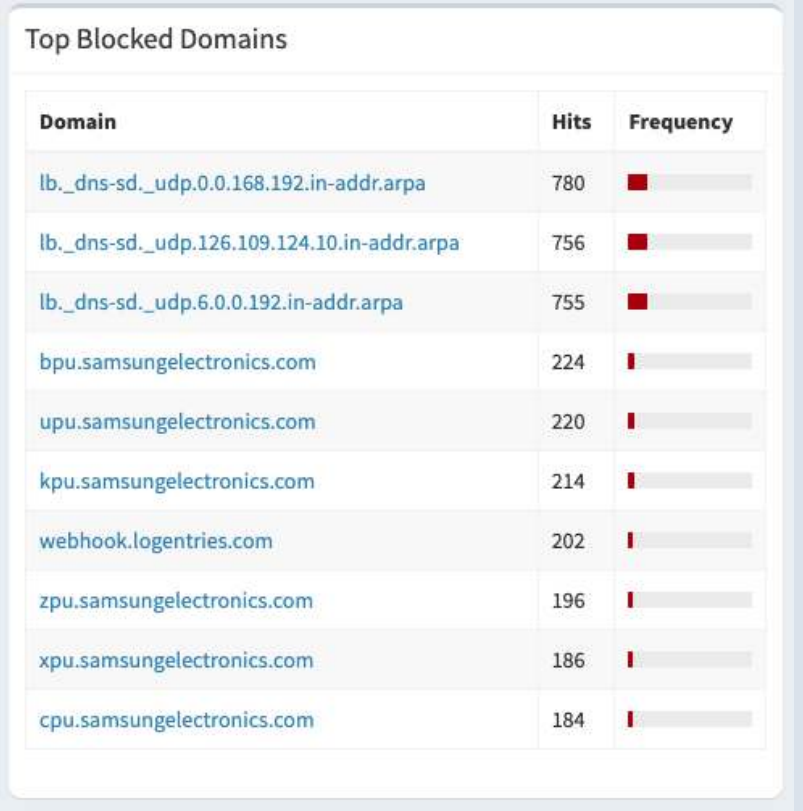



# DNS

Uso de algún "sumidero" o gestión de listas como Pi-hole https://pi-hole.net
Muy útil en casa con dispositivos "inteligentes" para bloquear rastreos o malware y como caché.
Ejemplos: https://avoidthehack.com/best-pihole-blocklists



# VPN

No navegas con tu IP, navegas con la salida del túnel que se crea desde tu dispositivo hasta el proveedor.
*“curl ifconfig.me”*

Lo importante es tener la certeza de que el proveedor de VPN no se dedica a analizar o almacenar tus conexiones.
Muchos proveedores te prometen falsa privacidad y seguridad. Los proxies no son VPN.

En Europa tenemos (entre otros):

- Proton https://protonvpn.com/
- Mullvad https://mullvad.net/es
- AirVPN https://airvpn.org
- SwissCows https://accounts.swisscows.com/products/vpn

Otra alternativa lowcost puede ser auto alojarlo:

- En casa, para cifrar nuestro tráfico cuando estemos fuera (sólo hasta casa)
- En un VPS en algún punto de Europa.

Inconvenientes de la VPN

- Detección de origen de un CPD https://www.24metrics.com/tools/ip-reputation-check/
- Restricciones de navegación por país

# Navegadores

✘Google Chrome, Microsoft Edge, ChatGPT Atlas, Comet, ...

Buscar alternativas como:

- Mullvad Browser https://mullvad.net/en/browser
- Vivaldi https://vivaldi.com/es/
- Firefox o LibreWolf https://librewolf.net/
- Brave (con la boca muy pequeña)
- Midori https://astian.org/midori-browser/
- Floorp https://floorp.app/en-US

TODOS los navegadores necesitan configuración después de instalarlos.
Es buena idea tener varios instalados según el uso.

Como prueba de si nuestra configuración filtra datos:
- https://coveryourtracks.eff.org
- https://ipleak.net

# Navegadores

Las extensiones acceden a tus datos en el navegador, cuantas menos mejor. Validar siempre el origen.

- Privacy Badger [https://privacybadger.org/es/]
- VPN
- uBlock Origin [https://ublockorigin.com/es]
- Firefox Multi-Account Containers
- User-Agent Switch
- Gestor de contraseñas

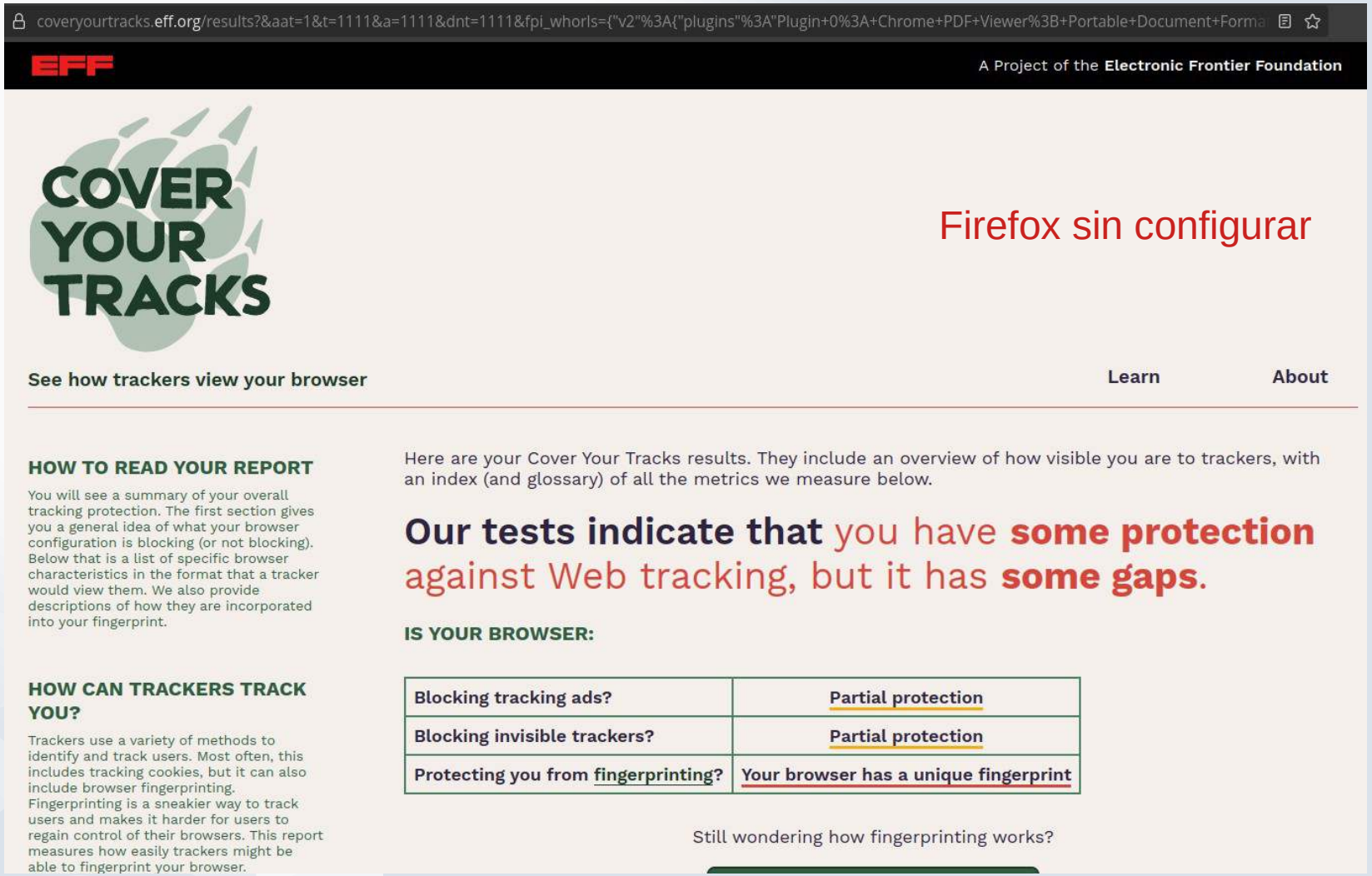
**Buscadores**

Los más conocidos recopilan datos sobre los usuarios como términos de búsqueda, historial de navegación, ubicación, dispositivos utilizados, entre otros para personalizar los resultados y mostrar publicidad dirigida.

Alternativas Europeas:

- www.startpage.com
- www.qwant.com
- www.ecosia.org
- swisscows.com
- metager.org

# Navegadores



# Navegadores

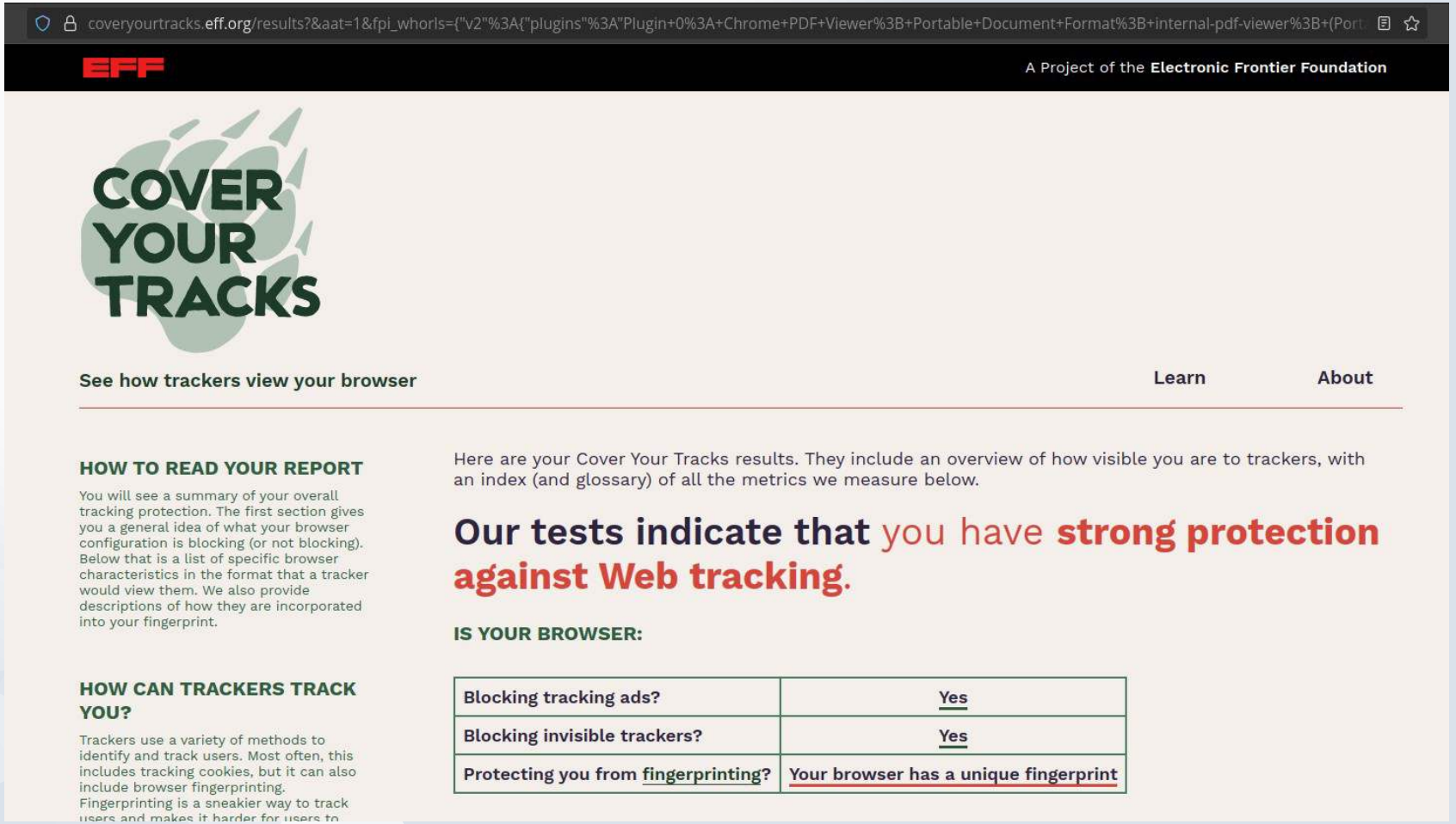
**Inicio**
- Desmarcar todo
- Pagina de inicio: blank page

**Búsqueda**
- Quitar las búsquedas sugeridas

**Privacidad y Seguridad**
- Proteccion contra rastreo -> Estricto
- Decir a los sitios web ... -> No
- Eliminar cookies ... -> Si
- Guardar contraseñas ... -> No
- Autocompletado -> No
- Historial -> Modo permanente de navegación privada
- Bloquear ventanas emergentes -> Si
- Advertirle cuando los sitios web intenten ... -> Si
- Recopilación y usos de datos de Firefox -> No
- Preferencias de publicidad -> No
- Seguridad -> Si a todo
- Certificados -> Si
- Modo solo-HTTPS -> Activar solo-HTTPS en todas las ventanas
- DNS sobre HTTPS -> Protección máxima ( https://dns.quad9.net/dns-query )


https://github.com/arkenfox/user.js

# Navegadores



# Gestor de contraseñas

**El block de notas no es un gestor de contraseñas. No repetir las contraseñas ni los usuarios.**

Con ellos solo tienes que aprenderte una contraseña, y las demás pueden ser todo lo complejas que quieras. Puedes añadir el 2FA.

A mi me gustan:

- Keepass https://keepass.info/
- KeepassXC https://keepassxc.org/
- Bitwarden https://bitwarden.com
  - Tiene versión auto-alojada https://github.com/dani-garcia/vaultwarden
- Proton Pass https://proton.me/es-es/pass

# Alternativas de correo electrónico

✘Gmail, Outlook, Yahoo, ... Están fuera de Europa, acceden a tu correo, alimentan sus IA, ...

Servicios en Europa:

- Proton.me https://proton.me
- Tuta.com https://tuta.com/es
- Mailbox.org (Para empresas) https://mailbox.org/en/
- Simplelogin (para hacer alias) https://simplelogin.io
- Swisscows https://swisscows.com/es/
- Starmail https://www.startmail.com/
- Gmx https://www.gmx.es
- Runbox https://runbox.com/

Usar dominios propios para controlar las cuentas, migrarlo, hacer backups, etc.
Cifrar los contenidos con PGP: https://www.incibe.es/empresas/blog/utiliza-el-correo-electronico-forma-segura-pgp

# Redes sociales

Las redes sociales son un negocio basado en la venta de publicidad alimentada por nuestros datos. Ya forma parte de las leyenda urbanas que las aplicaciones nos espían: “me puse a hablar de X y al día siguiente tenia Instagram lleno de anuncios”. Aplicaciones gratuitas se nutren de los datos de tu dispositivo: [https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html]

Además las aplicaciones de redes sociales están diseñadas para obtener la máxima información posible de nuestros dispositivos (localización, agenda, cuando estas conectado, que has visto, que no, etc).

Aunque no sea tan usable, es mejor usar el navegador con las máximas restricciones, para utilizar redes sociales. Podemos usar proxies para consultarlas puntualmente. https://farside.link/

La alternativa son las redes federadas (También conocidas como el Fediverso).  Esto significa que los servicios se componen de múltiples nodos interconectados pero independientes entre si. Cada nodo puede tener sus propias reglas aunque estén interconectados. En ocasiones puede ocurrir que desde nuestro nodo, no se puedan ver todos los contenidos de la red.

# Redes sociales

Mastodon
- https://joinmastodon.org/es
- https://social.vivaldi.net
- https://paquita.masto.host
- https://pleroma.social

Lemmy
- https://join-lemmy.org/?lang=es
- https://lemmy.world

Zoom:
- Teleguard https://teleguard.com/es
- Jitsy https://jitsi.org/

Pixelfed
- https://pixelfed.org/servers
- https://pixelfed.es
- https://fotolibre.social/

Friendica:
- https://friendi.ca

Video:
- https://joinpeertube.org
- https://loops.video

Mensajería:
- Signal.org/es
- Olvid https://olvid.io/en/
- XMPP https://xmpp.org/
- Delta Chat https://delta.chat/es/

# IA Alternativas

Las empresas de IA esta en una carrera de posicionamiento entre el usuario y la tecnología. A futuro tendremos dependencia e incremento de costes.

**LeChat Mistral** https://mistral.ai/terms#privacy-policy
**Lumo** https://lumo.proton.me/about
**Apertus** https://publicai.co (Public AI)
**Freepik** https://www.freepik.es
**Solidagent** https://www.solidagent.io
Auto alojados (no todos son opensource)

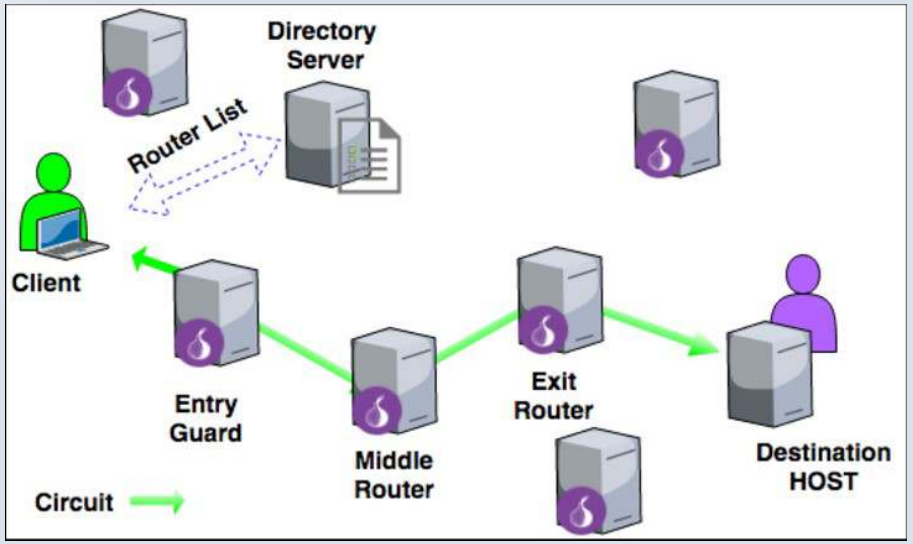
- Ollama  https://ollama.com/
- LMStudio  https://lmstudio.ai/
- AnythingLLM https://anythingllm.com
- Stable Diffusion en Local https://easydiffusion.github.io/
- Comfy UI para generar multimedia: https://www.comfy.org/
- Descargar modelos de HuggingFace y convertirlos a Ollama. https://danielmiessler.com/blog/how-to-use-hugging-face-models-with-ollama

# Uso de TOR

Tor es una red, que cifra por capas las comunicación entre sus nodos, de modo que cada nodo solo conoce el siguiente punto de destino.
Los dominios son .onion, solo se pueden ver conectados a esa red y su contenido no está indexado.

Pros:
- Permite navegar por Internet de forma anónima (hasta que hagas login en algún sitio)
- Enruta y cifra la conexión a través de una serie de servidores. Comprometer la red es muy costoso.

Cons:
- A los sitios web puede no gustarle y bloquear el tráfico de Tor
- Algunas páginas se rompen al bloquear scripts




Ejemplos:
- torproject.org: Usar el navegador TOR
- "Torificar" la conexión ProxyChains
- Whonix (Tor Gatway) https://www.whonix.org
- Tails OS https://tails.net

Algunos enlaces:
- https://check.torproject.org/
- https://thehiddenwiki.org
- http://nv3x2jozywh63fkohn5mwp2d73vasusjixn3im3ueof52fmbjsigw6ad.onion
- http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei4m6f7tayd.onion

# Otras redes

Hay otros proyectos de crear redes privadas sobre internet, que pueden ser útiles para proteger nuestras comunicaciones.

- **hyphanet.org**, antigua freenet
- **geti2p.net**, que una red p2p privada sobre internet
- **Mixnets**, que se caracterizan por:
  - Mensajería asíncrona
  - Seguridad contra análisis de tráfico
  - Acumula y mezcla

  Ejemplos:
  - **cMixx (xx.network)** https://xx.network/
  - **Katzenpost** https://katzenpost.network/
  - **Nym VPN** https://nym.com/

# Móviles

Alternativas reales:

- Fiarte de Apple
- Instalar Graphene OS en un Pixel
- Buscar un teléfono "Desguguelizado" (deGoogled) o tratar de crearlo
- Esperar a que sea el año de Linux en móvil

Las alternativas de Android se basan en el uso de librerías open source que simulan los servicios de Google como MicroG (GMSCore), para que las aplicaciones sigan funcionando. (https://github.com/microg)

- **Graphene OS**: ROM Android sobre móviles Pixel que ademas cifra el dispositivo. https://grapheneos.org
- **Volla OS**: Alemanes, Android sin Google o Ubuntu Touch. https://volla.online
- **Fairphone**: Holandeses, sostenibles. https://www.fairphone.com/
- **Murena:** Franceses, soluciones opensource. https://murena.com/es/

Roms alternativas. Útiles para actualizar dispositivos antiguos. Validar que funciona con MicroG y son compatibles.

- LinageOS (https://lineageos.org)
- CalyxOS (https://calyxos.org/)
- ParanoidAndroid (https://paranoidandroid.co)
- PixelExperience (https://get.pixelexperience.org)
- Havoc-OS (https://havoc-os.com/)

# Móviles

La opción "Low-cost" es buscar un terminal que lleva lo mas parecido a Android Stock y "desgugüelizarlo":

- Arrancar sin usar una cuenta de google.
- Instalar tiendas alternativas F-droid y Aurora. Con ellas instalar las aplicaciones que NO usen los servicios de google. https://f-droid.org/ y https://auroraoss.com/aurora-store
- Llamadas y agenda: https://github.com/FossifyOrg/Phone
- Teclado: https://anysoftkeyboard.github.io/ o https://github.com/Helium314/HeliBoard
- Fotos: https://github.com/deckerst/aves
- Correo: https://k9mail.app/
- Mapas: https://osmand.net/
- Notas: https://github.com/laurent22/joplin
- Cambiar el launcher: https://lawnchair.app/
- Recuerda remplazar las aplicaciones por defecto por las aplicaciones FOSS.

Lista completa: https://github.com/pluja/awesome-privacy?tab=readme-ov-file#android

# Eliminar metadatos

❯ exiftool -all= -overwrite fichero.pdf
❯ qpdf --linearize fichero_original.pdf fichero_destino.pdf

```
❯ exiftool fichero.pdf
ExifTool Version Number         : 13.36
File Name                       : fichero.pdf
Directory                       : .
File Size                       : 293 kB
File Modification Date/Time     : 2025:10:06 13:46:19+02:00
File Access Date/Time           : 2025:10:06 13:46:19+02:00
File Inode Change Date/Time     : 2025:10:06 13:46:19+02:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 3
Language                        : es
Tagged PDF                      : Yes
XMP Toolkit                     : 3.1-701
Creator                         : J**** ******
Creator Tool                    : Microsoft Word
Create Date                     : 2025:10:06 04:46:13-07:00
Modify Date                     : 2025:10:06 04:46:13-07:00
Document ID                     : uuid:1BAEECFC-8C46-4F60-BBE9-
**********
Instance ID                     : uuid:1BAEECFC-8C46-4F60-BBE9-**********
Author                          : J**** ******
```

```
❯ exiftool fichero.pdf
ExifTool Version Number         : 13.36
File Name                       : fichero.pdf
Directory                       : .
File Size                       : 293 kB
File Modification Date/Time     : 2025:10:06 13:46:59+02:00
File Access Date/Time           : 2025:10:06 13:46:59+02:00
File Inode Change Date/Time     : 2025:10:06 13:46:59+02:00
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 3
Language                        : Yes
Tagged PDF                      : Yes
```

# Otras alternativas europeas

Traducción
- DeepL https://www.deepl.com/en/translator
- Reverso https://www.reverso.net

Repositorio
- Codeberg https://codeberg.org
- GitLabHost https://www.gitlabhost.com

Streaming
- Mubi https://mubi.com/es/es
- Filmin https://www.filmin.es

Notas / Office
- Anytype https://anytype.io/
- Affine https://github.com/toeverything/AFFiNE
- Jopin https://joplinapp.org
- Cryptpad https://cryptpad.fr
- Disroot https://disroot.org/#services
- Onlyoffice https://www.onlyoffice.com/es/

Empleo
- Xing https://www.xing.com/es

Reuniones/chats
- JitsyMeet https://jitsi.org/jitsi-meet/
- Wereby https://whereby.com
- Stackfield https://www.stackfield.com
- Element https://element.io

Almacenamiento
- Koofr https://koofr.eu
- Filen.io https://filen.io
- Internxt https://internxt.com/

Linux:
- Open Suse (https://www.opensuse.org/)
- Linux Mint (https://linuxmint.com)
- Parrot Security OS https://www.parrotsec.org

# Egosurfing

En buscadores:

- allintext: “nombre apellidos”, “dni”, “+346xxxxxxxx”

Herramientas online:

- Epieos https://epieos.com/
- Have I been Pwned? https://haveibeenpwned.com/
- Cybernews https://cybernews.com/personal-data-leak-check/
- Dehashed https://dehashed.com/search#breachCheck

# Truquitos de andar por casa

- No rellenes todos los campos.
- Usa variaciones de tu nombre/alias en los registros.
- Crea una cuenta de correo para organismos oficiales o bancos y úsala solo ahí.
- Utiliza alias de correo por registro o una cuenta chorra para filtrar publicidad.
- No sincronices las agendas con aplicaciones de mensajería.
- No des tú numero de móvil, si no es necesario. Nada de grupos de Whatsapp con desconocidos.
- Ten una segunda linea, para publicidad o cosas que no te importan.
- Revisa las opciones de seguridad y privacidad de todas, repito: Todas tus aplicaciones.
- Cierra cuentas que no vayas a usar.
- Utiliza un navegador para cosas privadas/oficiales y otro para ocio.
- Cierra sesión siempre. Revisa en tus cuentas online que dispositivos/apps hay autorizados.
- Cambiar las aplicaciones por defecto en Android por aplicaciones libres.
- Haz egosurfing cuando puedas.

# Para saber más

Comparación de servicios VPN y Correo:

- https://thatoneprivacysite.xyz

Alternativas Europeas

- https://www.goeuropean.org
- https://european-alternatives.eu

Listado de software libre:

- https://github.com/pluja/awesome-privacy

Alternativas a aplicaciones:

- https://alternativeto.net

Blogs:

- https://mullvad.net/es/blog/tag/privacy-tips
- https://feliz1984.com
- https://www.startpage.com/privacy-please/

# Preguntas