# Manual de autodefensa en la era de la digitalización forzada

# o

# Resistencia al capitalismo de vigilancia

**Valentin Delacour**

**2017 - 2023**

# Índice

# 1. Introducción

## Problemática

En el marco dictado por el capitalismo de vigilancia, empresas privadas acumulan cantidades astronómicas de datos personales que cada persona transmite inconscientemente en permanencia, a través de toda actividad conectada. Dado su control hegemónico sobre los datos y sus algoritmos predictivos siempre más efectivos, la agrupación de cada dato particular, aparentemente sin interés por separado, permite constituir un panorama global de nuestro perfil psicológico y así prever nuestras reacciones, lo que les otorga el poder de influenciar nuestro comportamiento y, además de ejercer este poder de influencia, de venderlo al mejor postor. La necesidad de resistencia frente a ese sistema distópico de control social tan potente e insidioso, con consecuencias desastrosas para nuestras sociedades, trata, más allá del derecho personal a la privacidad, del interés colectivo de luchar para la dignidad humana, la libertad y en definitivo, una sociedad más sana.

## Objetivos del documento

Este documento se destina a todas las personas conscientes o tomando consciencia de la importancia de la privacidad y de la protección de los datos personales en nuestra sociedad, independientemente de sus conocimientos del tema. Tiene como objetivo principal proponer herramientas y alternativas para proteger los datos personales de la predación de empresas privadas. El documento pretende lograr un equilibrio entre recomendaciones pragmáticas e ideológicas pues la conjunción de las dos es necesaria para realmente defender la privacidad en nuestra sociedad de manera eficiente y duradera.
Más allá del modelo de amenaza establecido, un objetivo subsidiario es proporcionar recomendaciones garantizando la seguridad mínima necesaria, frente a los piratas informáticos en particular, sin la cual simplemente no se podría hablar de protección de datos. Accesoriamente, las siguientes recomendaciones permiten también reducir drásticamente las informaciones personales accesibles a los gobiernos mediante sus colaboraciones con el sector privado en matera de vigilancia.

En el afán de ayudar los lectores a elegir entre las diferentes opciones recomendadas, se propone una primera priorización (orden de aparición y presencia o no de paréntesis) subjetiva basada en la relación privacidad/usabilidad. Una segunda priorización (colores) se basa unicamente en la privacidad estimada : verde (verdadero respeto de la privacidad), azul (respeto de la privacidad bajo condiciones o presencia de elementos problemáticos en cuanto a la privacidad o seguridad), rojo (no protege o no respeta la privacidad pero sigue siendo preferible a las opciones de los MAGMAT) e incoloro (dependencia de factores externos). La presencia de un asterisco indica que la opción mencionada todavía no está madura en su estado actual.

**Advertencias**

Este documento, al tener como modelo de amenaza el capitalismo de vigilancia, no se destina a las personas necesitando una seguridad máxima o un anonimato total de parte de su función a riesgos tales como opositores políticos o algunos periodistas, aún si algunas opciones propuestas les convendrían. Efectivamente, el respeto de la privacidad no requiere necesariamente la imposibilidad de identificar al usuario.

El propósito del documento siendo proponer las soluciones más reputadas y prácticas sin estar sobrecargado, en el afán que su consulta permanezca lo más fácil y eficiente posible, no tiene por vocación ser exhaustivo. Dado que este enfoque impide detallar explicaciones para la mayoría de los elementos presentados, se invita a los lectores a buscar cualquier información adicional necesaria por sí mismos o en los recursos adicionales mencionados en el punto 8 del documento.

Varios meses después de la presente versión del documento, ciertas informaciones dadas serán obsoletas. El documento siendo actualizado frecuentemente, se les invita a conseguir la última versión en la página siguiente: “https://codeberg.org/PrivacyFirst/Data_Protection/issues”. Se agradece usar este enlace para compartir el documento en vez del archivo PDF, de tal manera que la ultima versión siempre esté accesible.

Este trabajo, aunque siendo el fruto de una experiencia y sobre todo de un aprendizaje largo de varios años basándose en innumerables contenidos e intercambios, y por lo tanto sin poder comportar fuentes como tales, permanece obviamente perfectible. Cualquier sugerencia o comentario es por lo tanto más que bienvenido al correo : “privacyfirst@ik.me”. Espero que este documento les ayudará a defender su privacidad y la de otros, en el afán de luchar para una sociedad más sana.

## 2. Glosario

| | |
|---|---|
| MAGMAT: | **M**eta (Facebook, etc.), **A**mazon, **G**oogle, **M**icrosoft, **A**pple y **T**witter |
| Código abierto: | código fuente públicamente disponible y así mismo verificable |
| Libre / FLOSS: | software de código abierto que puede ser libremente usado, modificado y redistribuido por todos |
| Propietario: | antónimo de libre, cuyo código no está publico ni modificable |
| P2P: | par a par (*Peer-to-peer*), pues sin servidor externo intermediario |
| Tor: | cf. 6.2 |
| Cliente: | programa que se conecta a un servicio (servidor) y sirve de interfaz |
| Proxy/proxies: | cf. 7.1 |
| ZKE: | *Zero-Knowledge Encryption*, cifrado de los datos en un servidor, de tal manera que solo el usuario pueda decifrarlos |

## 3. Reglas de oro

1. Evitar usar servicios y programas de los MAGMAT, al igual que chinos (TikTok, etc.), siempre que sea posible. Lo más recomendable es eliminar sus eventuales cuentas y reemplazarlas por alternativas respetuosas recomendadas en este documento.

2. Siempre revisar todos los ajustes y permisos de lo que se utiliza y optimizarlos para limitar al máximo la recolección de datos personales.

3. Usar programas o aplicaciones libres o de código abierto en vez de los propietarios de código cerrado siempre que es posible dado que sus códigos son públicos y así mismo verificables. Pensar en favorecer las opciones populares a las desconocidas puesto que serán más revisadas por la comunidad y, por lo tanto, confiables.

4. Solo instalar los programas o aplicaciones necesarios y privilegiar las Web Apps o los atajos desde el navegador para acceder a servicios en vez de aplicaciones propietarias a instalar para limitar las posibilidades de recolección de datos personales y las potenciales brechas de seguridad explotables en sus dispositivos.

5. Si una empresa propone sus servicios gratuitamente, en general, el producto que vende es usted (sus datos personales). Por causa del modelo impuesto por el capitalismo de vigilancia, pagar ya ni siquiera les protege de también ser el producto.

6. Actualizar sus programas y sistemas operativos frecuentemente para beneficiar de los últimos parches de seguridad y reemplazar los que ya no reciben actualizaciones.

7. No usar antivirus terceros, son verdaderas aspiradoras de datos personales (a parte de ClamAV). Su aporte es desdeñable con buenos hábitos numéricos. Una buena configuración y la prudencia son los mejores antivirus.

8. Usar un gestor de alias para correo o correos temporales para crear cuentas para ciertos servicios o plataformas en el afán de evitar dar su propia dirección de correo.

9. Siempre desactivar el Wi-Fi, Bluetooth y geolocalización de su smartphone cuando no se utilizan y no conectarse a Wi-Fi públicos sin el uso de una VPN.

10. No usar objetos conectados pues su propósito es recolectar la mayor cantidad posible de datos personales, o no conectarlos a internet cuando son imprescindibles.

11. Nunca usar soluciones de pago sin contacto concebidas para controlar, vigilar y analizar las transacciones de manera global. Pagar en efectivo es un acto militante para la defensa de la libertad y de la privacidad.

## 4. Servicios, aplicaciones y programas

Las recomendaciones se dividen, si procede, entre las que se pueden acceder desde el navegador, las aplicaciones Android (e iOS solo en caso de diferencia notable con las otras categorías) y los programas para computadora. Las aplicaciones y programas propuestos son libres, a menos que se especifique expresamente lo contrario. La priorización y los colores son explicados en la introducción.
Las aplicaciones propuestas para Android y derivados se deben buscar primero en la tienda respetuosa de aplicaciones libres Neo Store (F-Droid) y, solo si no están ahí, en Aurora Store, un cliente respetuoso de Google Play permitiendo tener acceso a sus aplicaciones gratuitas sin cuenta Google. Por favor véase el punto 9.2 para todas las explicaciones necesarias.

### Navegación y comunicación

Navegador (cf. 6)

Android: Mull(cf. 9.2), Tor Browser(cf. 6.2), (Bromite(cf. 9.2)), ((Privacy Browser)).
Ordenador: Firefox(cf. 9.5), LibreWolf(cf. 9.4), Tor Browser(cf. 6.2), (Brave), ((Ungoogled Chromium*)).
iOS (Safari): Brave, Onion Browser(cf. 6.2), (Firefox Focus).

Buscador

Navegador: SearXNG(cf. 7.1), Brave Search(cf. 9.4), (DuckDuckGo, Mojeek), ((Qwant, Swisscows, Startpage(proxy Google))).

Mensajería instantánea

Android: Threema Libre(cf. 9.2), Molly(Signal)(cf. 9.2), Session F-Droid*, SimpleX Chat*(cf. 9.2), (Jami*, Element, Telegram FOSS(cf. 9.2), Cwtch*, Briar).
Ordenador: Threema, Signal, Session*, (Jami*), ((Element, Cwtch*, Briar*)).

Videoconferencia

Navegador: Jitsi Meet(cf. 7.2), BigBlueButton(cf. 7.2), Threema, (Element, Telegram).
Android: Jitsi Meet(cf. 7.2), Jami*, Threema Libre(cf. 9.2), Molly(Signal)(cf. 9.2), (Element, Telegram FOSS(cf. 9.2)).
Ordenador: Jami*, Threema, Signal, (Element, Telegram).

Correo

Navegador: Proton Mail, Tutanota, mailbox.org, (Disroot(sin ZKE)).
Android: Proton Mail, Tutanota, K-9 Mail, FairEmail.
Ordenador: Thunderbird, GNOME Evolution, Kontact(KDE).

Gestor de alias para correo y correo temporal

Navegador: SimpleLogin, forwardemail.net, mailhole.de, (temp-mail.org).
Android: AnonAddy for Android, SimpleLogin.

**Plataformas y servicios**

Plataforma video

Navegador: Piped(proxy YouTube)(cf. 7.1), PeerTube, (Librarian(proxy Odysee/LBRY) (cf. 7.1), Invidious(proxy YouTube)(cf. 7.1)).
Android: LibreTube(proxy YouTube)*(cf. 7.1), Newpipe(YouTube/PeerTube)(cf. 9.2).
Ordenador: LBRY, FreeTube(YouTube)(cf. 9.4)).

Traducción

Navegador: DeepL(pago/gratuito), LibreTranslate, simplytranslate.org(multiproxy), (DuckDuckGo(proxy Microsoft), Apertium, Lingva Translate(proxy Google)).
Android: Translate You(multicliente), DeepL, Translate You Libre(LibreTranslate).
Ordenador: Firefox Translations(extensión)*, Argos Translate, Dialect(multicliente).

Mapas y GPS

Navegador: OpenStreetMap, Qwant Maps, DuckDuckGo,
Android: Organic Maps, OsmAnd+, Magic Earth(propietario), (Alpi Maps).
Ordenador: Organic Maps, Maps(GNOME), Marble(KDE).

Red social respetuosa

Navegador: Mastodon, Element, Telegram, PixelFed, Lemmy, (Pleroma, Friendica).
Android: Megalodon(Mastodon), Element, Telegram FOSS (cf. 9.2), Fedilab(multicliente), PixelDroid(PixelFed)*, Lemmur(Lemmy).
Ordenador: Element, Telegram.

Red social abusiva (cf. 7.1)

Navegador: Nitter(proxy Twitter), Libreddit(proxy Reddit), ProxiTok(proxy TikTok), Quetre(proxy Quora).
Android: Fritter(Twitter sin cuenta), Shitter(Twitter), Nitter for Android, Infinity for Reddit, Twire(Twitch), Navegador internet(Instagram, etc.).

Películas y series en linea

Android: CloudStream, Burning-Series, Kodi.
Ordenador: Stremio(sin cuenta/con cuenta)(propietario), Kodi.

Otras plataformas y servicios

Organización de eventos: Mobilizon
Plataforma de aprendizaje: Moodle, ILIAS, Canvas.
Ecosistema todo en uno: Proton, Skiff, Infomaniak(sin ZKE).

**Privacidad y seguridad**

Bloqueador de publicidad/rastreadores y DNS cifrado

Android: RethinkDNS*(cf. 9.2), (InviZible Pro, DoT de Android(cf. 9.1)).
Ordenador: Safing Portmaster
iOS: DNSCloak, DNS de iOS.

Gestor de contraseñas

Android: KeePassDX, Bitwarden(cf. 9.2).
Ordenador: KeePassXC, Bitwarden.
iOS: Strongbox(KeePass), Bitwarden.

Autentificación a dos factores

Android: Aegis, KeePassDX.
iOS: Tofu Authenticator, Raivo OTP.

Antivirus
Navegador: virustotal.com
Android: Hypatia(ClamAV)
Ordenador: ClamTK(Linux), ClamWin(Windows).

VPN (cf. 8)

Android: Mullvad VPN, Proton VPN, IVPN, (Riseup VPN, Calyx VPN).
Ordenador: Mullvad VPN, Proton VPN, IVPN.

Monitor de trafico de red y cortafuegos

Android: RethinkDNS*, (NetGuard).
Ordenador: Safing Portmaster, (Wireshark).

Otras aplicaciones para Android

Redirector y limpiador de enlaces (abusivo => respetuoso): UntrackMe(cf. 7.1 y 9.2)
Revelador de rastreadores terceros: ClassyShark3xodus, Exodus privacy, TrackerControl.
Anonimización red por Tor: Orbot: Tor for Android, InviZible Pro.
Desenfoque para fotografías: PrivacyBlur
Supresión de metadatos: ExifEraser, Scrambled Exif.
Aislador de aplicaciones: diferente perfil usuario de Android(cf. 9.1), Insular, Shelter.
Bloqueador (o monitor) de micrófono: PilferShush Jammer, (Vigilante).

Otros programas para ordenador

Gestor de permisos para programas Flatpak (Linux): Flatseal
Desenfoque o resistencia al reconocimiento facial: PrivacyBlur, Fawkes(SANDLab).
Supresión de metadatos: Metadata Cleaner, ExifCleaner.
Convertidor de archivos potencialmente peligrosos: dangerzone.rocks

**Productividad**

Agenda

Android: Proton Calendar, Simple Calendar Pro, Tutanota, Etar.
Ordenador: Proton Calendar, Tutanota, Calendar(GNOME), Kalendar(KDE).

Ofimática y colaboración

Navegador: CryptPad, Skiff, Collabora Online(profesional), (ONLYOFFICE Docs (profesional)).
Android: Collabora Office(LibreOffice)(cf. 9.2)
Ordenador: ONLYOFFICE, LibreOffice, (Collabora Office(LibreOffice profesional)).

Notas

Android: Notesnook, Noto*, SilentNotes, Joplin, jtx Board, Quillpad*, Orgzly, Nextcloud Notes, Obsidian(propietario).
Ordenador: Notesnook, Joplin, SilentNotes, Knotes(KDE), Gnote(GNOME), QOwnNotes, Notejot, Obsidian(propietario).

Lector PDF

Android: Secure PDF Viewer, MuPDF Viewer.
Ordenador: Sumatra PDF, Okular(KDE), Evince(GNOME).

Agregador de noticias (lector de flujo RSS)

Android: Feeder, Thud, (Read You*, News*).
Ordenador: Fluent Reader, Akregator(KDE), Feeds(GNOME), RSS Guard.

**Gestión de archivos y datos**

Transmisión de archivos

Navegador: send.vis.ee(< 2.5 GB), send.zcyph.cc(< 20 GB), (upload.disroot.org(< 2 GB), Tresorit Send(< 5 GB)).
Android: Syncthing(P2P), Warpinator(local), (Sharik(local)).
Ordenador: Syncthing(P2P), OnionShare(Tor), Warpinator(local), (Sharik(local)).

Cloud

Navegador: Proton Drive, ente.io(galería), Filen, Nextcloud(autoalojado), (kDrive(sin ZKE)), ((Disroot(sin ZKE), Cozy Cloud(sin ZKE))).
Android: Proton Drive*, ente(galería), Filen, Nextcloud(autoalojado), (kDrive(sin ZKE)).

Herramienta de sincronización y copia de respaldo

Android: Syncthing(P2P), DAVx[5](servidor elegido), (DataBackup*).
Ordenador: Syncthing(P2P), Déjà Dup(local)

Herramienta de cifrado

Android: Cryptomator
Ordenador: Picocrypt, VeraCrypt, Cryptomator, PeaZip.

Conexión entre smartphone y ordenador

Android: KDE Connect, Zorin Connect.
Ordenador: KDE Connect, GSConnect(GNOME), Zorin Connect.

**Otras aplicaciones para Android**

Reemplazo de aplicaciones de origen

Teclado: FlorisBoard*, (OpenBoard).
Cámara: Secure Camera, (Simple Camera).
Galería: Simple Gallery Pro, Photok, Les Pas(Nextcloud).
Gestor de archivos: Simple File Manager Pro, Material Files, Ghost Commander.
SMS: Simple SMS Messenger
Clima: OSS Weather, Geometric Weather, Clima, Weather.
Reproductor audio: Metro, (Music Player GO*, Auxio*).
Contactos: Simple Contacts Pro, OpenContacts.
Grabador audio: Simple Voice Recorder
Gestor de llamadas telefónicas: Simple Dialer
Calculadora: OpenCalc, Simple Calculator.
Reloj: Simple Clock
Reproductor multimedia: VLC, Kodi.
Launcher: Neo Launcher*, Simple Launcher*, Discreet Launcher, KISS Launcher.

Misceláneos

Creador de Web Apps: Mull, Bromite.
Escáner de códigos QR: Secure Camera, (Simple QR, QR Scanner (PFA)).
Gestor de podcasts: AntennaPod, News*.
Radio internet: Transistor – Simple Radio App

Streaming de música: Finamp(Jellyfin), Subtracks(Subsonic), Musify(YouTube).
Lector de libros electrónicos: KOReader.
Interfaz respetuosa para aparatos conectados: Gadgetbridge
Financias: Unstoppable Wallet, Sushi, Finance Manager (PFA), MoneyBuster.
Actividades físicas: Feeel – home workouts, Massive, OpenTracks, FitoTrack.
Salud: drip(menstruations), openScale, Pain Diary (PFA).
Emulador de consolas: Lemuroid*

**Otros programas para computadora**

Multimedia

Reproductor audio: Lollypop, Elisa(KDE), Rhythmbox, Audacious, Strawberry, Music(GNOME).
Reproductor multimedia: mpv, VLC, Kodi.
Streaming de multimedia (auto alojado): Jellyfin, Subsonic.
Edición de imágenes y dibujo: GIMP, Krita, Drawing(GNOME), KolourPaint(KDE).
Procesamiento de fotografías: Darktable, RawTherapee.
Edición gráfica vectorial: Inkscape, Karbon(KDE).
Maquetación de páginas: Scribus
Edición audio: Audacity, Ardour, LMMS.
Edición video: Kdenlive, Pitivi, OpenShot, Blender, Avidemux, Shotcut.
Grabación de CD/DVD: Brasero(GNOME), K3b(KDE).
Transcodificación: Handbrake, MKV.

Misceláneos

Programas/juegos Windows en Linux: PlayOnLinux(Wine), Wine, (WinApps*).
Limpieza y optimización de sistema: Stacer, BleachBit.
Radio internet: Shortwave(GNOME), Radiotray-NG, Elisa(KDE), Lollypop.
Emulador de consolas: Higan, SameBoy, Dolphin, PCSX2, Nestopia UE, PPSSPP, DeSmuME.
Emulador de sistema operativo (virtualización): KVM, VirtualBox, Boxes(GNOME).

# 5. Sistemas operativos

## 5.1 Smartphone

Android, en su configuración por defecto, es actualmente el peor sistema operativo en cuanto a la privacidad. Su propósito es transmitir continuamente datos personales hacia los servidores de Google en el afán de explotarlos. La solución más recomendable en la actualidad es usar una versión de Android modificada (*custom ROM*) y "degooglizada" para respetar la privacidad. Sin embargo cuidado, la gran mayoría de los equipos (exceptuando los Pixel y OnePlus) y de las *custom ROMs*, tales como LineagesOS y sus derivados (a parte de DivestOS), no son adaptados para beneficiar del arranque verificado al volver a cerrar el *bootloader* luego de la instalación. Esto representa una brecha de seguridad.
Si no desean instalar un sistema operativo respetuoso y que a pesar de todo desean usar Android de origen, sigan los consejos detallados en el punto 9.1 de este documento en el afán de limitar al máximo la recolección de datos personales.
El sistema operativo de Apple (iOS), a pesar de su marketing basado en el respeto de la privacidad, también recolecta y explota los datos personales de sus usuarios además de limitar considerablemente su libertad.
Las opciones basadas en Linux son respetuosas de la privacidad y prometedoras en términos de independencia pero no ofrecen las mismas garantías en términos de seguridad que Android. Además, en su estado de desarrollo actual, no son recomendables para usuarios promedios.

### Android modificado para la privacidad

GrapheneOS (cf. 9.1): el Android degooglizado más seguro y privado disponible
DivestOS: LineageOS degooglizado y mejorado para la seguridad y privacidad
(CalyxOS) (cf. 9.1): Android parcialmente degooglizado pero con microG
(iodéOS) (cf.9.1): LineageOS parcialmente degooglizado con microG (desinstalable)
(/e/OS) (cf. 9.1): LineageOS parcialmente degooglizado con microG y servicios cloud
((LineageOS for microG)): LineageOS con microG para una mejor compatibilidad
((LineageOS)): Android sin Google apps pero no degooglizado

microG es una implementación libre pero imperfecta de los servicios Google Play cuyo propósito es compensar la falta de compatibilidad de las versiones "degooglizadas" de Android con las aplicaciones abusivas dependientes de estos últimos. Realiza por defecto conexiones directas hacia los servidores de Google y se cuestiona sus implicaciones en términos de seguridad.

### Hardware

La casi totalidad de los smartphones vendidos nuevos con una versión de Android degooglizada tienen lamentablemente procesadores cuyo soporte venció o está a punto de vencer y los vendidos de segunda mano vienen generalmente con el bootloader abierto. Los problemas de seguridad que eso implica vuelven entonces una tal inversión desacertada. Se recomienda, en su lugar, adquirir un Pixel (6 o superior) de segunda mano, en el afán de no soportar económicamente Google, cuyo bootloader no está bloqueado (evitar los vendidos por operadoras) e instalar GrapheneOS cuyo proceso de instalación automatizado desde su página oficial está bien documentado y al alcance de todos. Esto permite beneficiar de los mejores SO y hardware en términos de seguridad y privacidad, y posiblemente de manera más económica.

## 5.2 Ordenador

Windows (cf. 9.3) actualmente es el peor sistema operativo en términos de privacidad. Los únicos sistemas operativos de fácil uso que, al contrario de macOS, respetan realmente la privacidad son las distribuciones libres GNU/Linux (cf. 9.3). Existe una multitud cuyas características varían considerablemente. Aquí una pequeña selección de las distribuciones ofreciendo la mejor experiencia para el usuario (siempre respetando la privacidad) o garantizando la mayor protección de datos.
Cabe recordar que cada una de ellas propone una o varias interfaces (entornos de escritorio) diferentes en términos de experiencia de usuario y de consumo de recursos. Por motivos de seguridad, privilegien uno que soporte Wayland tal como GNOME o KDE Plasma. Existe una abundante documentación en linea para identificar cual distribución y entorno de escritorio convendrán mejor a las capacidades de su computadora y a sus preferencias así como para saber como instalarla fácilmente.

### Ordenador

Fedora Workstation: estándares seguros y modernos
Linux Mint: ideal para los principiantes y gran estabilidad
Zorin OS: ideal para los principiantes acostumbrados a Windows o macOS
Pop!_OS: ideal para los principiantes
MX Linux (cf. 9.3): liviana y gran estabilidad (conviene a los principiantes)
(Parrot): opción de anonimato global por Tor (liviana)
(Fedora Silverblue*): alta seguridad y estándares modernos (centrado en Flatpak)
(Qubes OS): seguridad extrema para usuarios avanzados (alto consumo de recursos)
(Whonix): anonimato global por Tor y seguridad extrema (usar en KVM o VirtualBox)

### USB live (RAM)

MX Linux: liviana y gran estabilidad (opción de persistencia)
Tails: anonimato global por Tor y no deja rastros en el equipo

### Raspberry Pi

LibreELEC: centro multimedia para TV (Kodi)
Batocera: emulador (videojuegos) y centro multimedia para TV (Kodi)
Raspberry Pi OS: sistema operativo clásico
MX Linux: sistema operativo clásico
(Plasma BigScreen*): interfaz multimedia para TV (comando de voz con Mycroft AI)

### Hardware

Las marcas siguientes venden ordenadores con Linux preinstalado:

| | |
|---|---|
| Slimbook | Vant |
| Librem | PINE64 |
| TUXEDO Computers | System 76 |
| Laptop with Linux | Entroware |
| Juno Computers | Vikings |
| Dell (unos modelos) | ThinkPenguin |

También existen otros vendedores menos conocidos de ordenadores con Linux preinstalado. En cuanto a los vendedores de ordenadores con Windows preinstalado, los modelos de Dell, Asus, Lenovo y HP son reputados por tener una buena compatibilidad con Linux. Es recomendable evitar comprar ordenadores que vienen con una tarjeta gráfica Nvidia dado que son conocidas por padecer de problemas de compatibilidad.

## 6. Navegadores

La compartimentalización (usar diferentes navegadores con diferentes configuraciones, según las tareas) es un método recomendado para preservar la privacidad sin sacrificar demasiado la comodidad de navegación.
Por ejemplo, se trataría de usar Firefox con una configuración protectora (cf. 9.5) para la navegación general. Luego, usar LibreWolf, u otro perfil del mismo Firefox configurado de manera menos restrictiva, para los sitios que requieren una conexión a una cuenta personal y también un navegador basado en Chromium tal como Brave o Ungoogled Chromium para la consulta de los sitios más recalcitrantes a la protección de la privacidad que no cargan correctamente. También es concebible usar un navegador unicamente dedicado al e-banking y Tor Browser para la navegación anónima.

### 6.1 Extensiones

Las extensiones son complementos que sirven para añadir funciones al navegador. Se recomienda instalar la menor cantidad posible y unicamente las confiables dado que pueden tener acceso a la totalidad de su navegación y que su uso puede ser identificado por las páginas web y servir para el rastreo (fingerprinting). Algunas de las siguientes extensiones recomendadas solo están disponibles para Firefox y LibreWolf. Sus diferentes configuraciones son detalladas en el punto 9.5.

| | |
|---|---|
| Protección de la privacidad: | uBlock Origin, LocalCDN, LibRedirect. |
| Según el uso: | KeePassXC o Bitwarden, Firefox Translations*. |

### 6.2 Tor Browser

El concepto de Tor es hacer pasar el trafico internet por una red anonimizandolo. En el afán de que la huella (fingerprint) de su navegador (dada entre otros por su configuración) no traicione su identidad por su singularidad, los navegadores Tor son concebidos para tener la misma huella independientemente de los usuarios. Para evitar volver única la huella de su navegador Tor, es recomendado evitar instalar extensiones y realizar modificaciones en los ajustes "about:config". Si se desea preservar el anonimato proporcionado, también es necesario no conectarse a cuentas que podrían de facto anularlo.
El método de anonimización de la red Tor ralentiza las cargas. Pues no es recomendado usarlo para el streaming o las descargas voluminosas.

## 7. Instancias de servicios

### 7.1 Proxies

Los proxies siguientes son intermediarios entre las plataformas abusivas y el usuario. Permiten tener acceso a su contenido sin entregarles informaciones personales. Sin embargo, sus diferentes instancias no ofrecen las mismas garantías de respeto de la privacidad (log de dirección IP o no, etc.). Se recomienda usar la extensión LibRedirect (cf. 9.5) en el afán de redirigir automáticamente los enlaces de plataformas abusivas hacia un proxy respetuoso y de distribuir la actividad entre varias instancias del mismo para evitar que una sola tenga acceso a todo el contenido consultado. Al usar el smartphone, se recomienda usar la aplicación UntrackMe (cf. 9.2).
Con respecto a las instancias de Nitter (Twitter), Libreddit (Reddit), ProxiTok (TikTok) y Quetre (Quora), por favor referirse directamente a las listas incluidas en LibRedirect y UntrackMe.

#### SearXNG

SearXNG es un metabuscador libre que proporciona los resultados combinados de varios buscadores (Brave Search, Google, Bing, etc.) sin transmitirles datos personales. Permite, si uno lo desea, una configuración particularmente avanzada.
Ahí una selección de las instancias más recomendables :

| | | |
|---|---|---|
| Sin log de dirección IP: | https://www.gruble.de | (Alemania) |
| | https://search.sapti.me | (Alemania) |
| | https://search.disroot.org | (Países Bajos) |

#### Plataformas video

Piped e Invidious dan acceso al contenido de YouTube sin entregar los datos personales del usuario a Google. En el caso de Invidious, el proxy escondiendo la dirección IP no está activado por defecto. Es posible activarlo manualmente en los ajustes de la instancia. En cuanto a Librarian, da acceso al contenido Odysee/LBRY que también es una plataforma abusiva. Sin embargo cuidado, la mayoría de sus instancias no son proxies.
A continuación, las diferentes instancias recomendadas, sin log de dirección IP :

| | | |
|---|---|---|
| Piped: | https://piped.adminforge.de | (Alemania) |
| | https://piped.projectsegfau.lt | (Francia) |
| Librarian (proxy activado): | https://lbry.projectsegfau.lt | (Francia) |

## 7.2 Videoconferencia

### Jitsi Meet

| | | |
|---|---|---|
| Log IP, versión pro opcional: | https://fairmeeting.net | (Austria) |
| Sin log de dirección IP: | https://calls.disroot.org | (Países Bajos) |
| | https://teamjoin.de | (Alemania) |
| | https://meet.rollenspiel.monster | (Alemania) |
| Log IP “anonimizado” temporal: | https://vc.autistici.org | (Alemania) |
| Log IP temporal: | https://meet.calyx.net | (EE. UU.) |

### BigBlueButton

| | | |
|---|---|---|
| Log de dirección IP: | https://meet.nixnet.services/b | (EE. UU.) |
| | https://bbb.fdn.fr/b | (Francia) |

## 7.3 Servidores DNS

Se recomienda usar un servidor DNS cifrado respetuoso, entre las recomendaciones a continuación, gracias a herramientas tales como RethinkDNS (cf. 9.2) para Android y Portmaster (cf. 9.4) para ordenadores, o bien con la solución nativa de su sistema de explotación. Si usan una VPN, es recomendable no cambiar el servidor DNS por defecto de esta última, en el afán de no destacar de sus otros usuarios.

AdGuard: bloqueo publicidad, rastreadores y dominios maliciosos (intercontinental)
DoH: https://dns.adguard.com/dns-query
DoT: dns.adguard.com
DoQ: quic://dns.adguard-dns.com

Mullvad: bloqueo publicidad, rastreadores y dominios maliciosos (intercontinental)
DoH: https://adblock.doh.mullvad.net/dns-query
DoT: adblock.doh.mullvad.net

BlahDNS: bloqueo publicidad, rastreadores y dominios maliciosos (Europa y Asia)
Control D: bloqueo publicidad, rastreadores y dominios maliciosos (intercontinental)
Quad9: bloqueo dominios maliciosos (intercontinental)
NextDNS: bloqueo personalizable (intercontinental)

## 8. Recursos adicionales

### Informaciones generales

Excelentes recursos para comprender el capitalismo de vigilancia y sus amenazas:
- *Nothing to Hide*, Marc Meillassoux (documental)
- *El dilema de las redes sociales*, Jeff Orlowski (documental de divulgación)
- *La era del capitalismo de la vigilancia*, Shoshana Zuboff (libro)
- *Diez razones para borrar tus redes sociales de inmediato*, Jaron Lanier (libro)

Excelente cadena anglófona acerca de la privacidad:
- The Hated One (LibreTube, Newpipe, Piped o Invidious)

Asociaciones para la defensa de la privacidad:
- https://www.derechosdigitales.org
- https://r3d.mx
- https://www.laquadrature.net/es
- https://www.eff.org/deeplinks (anglófono)
- https://privacyinternational.org (anglófono)

### Informaciones especificas

Excelentes tutoriales para la privacidad y la protección de datos:

completo:
- https://ssd.eff.org
- https://privacyguides.org (anglófono)
- https://dt.gl/privacy-cookbook-the-story-so-far-april-2022 (anglófono)

Avanzado:
- https://privsec.dev (anglófono, enfoque seguridad)
- https://anonymousplanet-ng.org (anglófono, enfoque anonimato)

básico:
- https://spreadprivacy.com/tag/device-privacy-tips (anglófono, sesgo pro DuckDuckGo)
- https://www.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide (anglófono, sesgo pro Apple)

Android y derivados:
- La excelente documentación de GrapheneOS: https://grapheneos.org/faq
- DivestOS: https://divestos.org
- Compatibilidad de las aplicaciones con y sin microG: https://plexus.techlore.tech

Configuración Firefox y derivados (anglófono):
- https://librewolf.net/docs/faq
- https://github.com/arkenfox/user.js/wiki

Utilidad y limitaciones de las VPN (anglófono):
- https://www.ivpn.net/blog/why-you-dont-need-a-vpn
- https://www.doineedavpn.com

Comparativos de proveedores de internet/operadores:
https://www.eff.org/pages/quien-defiende-tus-datos

**Servicios**

Asociaciones proponiendo excelentes servicios respetuosos de la privacidad:
- https://disroot.org/es
- https://adminforge.de/services
- https://framasoft.org/es
- https://projectsegfau.lt/instances
- https://www.nobigtech.es

Evaluación del respeto de la privacidad de diferentes servicios (anglófono):
- https://privacyspy.org (anglófono)
- https://tosdr.org

Herramienta de evaluación de seguridad de sitios web (anglófono):
- https://observatory.mozilla.org (anglófono)

**Grupos de privacidad y software libre**

Telegram:
- t.me/privacidadlibre (sala de entrada para el grupo privado)
- t.me/privateyourtech (anglófono)
- t.me/grupo_telegram_proyectotictac

Matrix:
- #privacidadlibre:matrix.org
- #privacy:matrix.org (anglófono)
- #main:privacyguides.org (anglófono)

# 9. Configuraciones

## 9.1 Sistemas operativos para smartphones

### Recomendaciones globales para Android y derivados

- cf. 4 y 9.2 para poder instalar aplicaciones sin Google Play Store

- revisar todos los permisos de las aplicaciones para retirarlos si son nefastos para la privacidad o innecesarios:
“Configuración” > “Apps” > seleccionar la aplicación > “Permisos”

- bloquear el acceso internet de todas las aplicaciones no usadas o que no requieren un acceso internet para funcionar en los permisos de las aplicaciones o, cuando no esta disponible, gracias a una aplicación cortafuegos como RethinkDNS

- instalar y usar una aplicación, como RethinkDNS (cf. 9.2), que permite bloquear los rastreadores así como la publicidad y usar un servidor DNS respetuoso cifrado (cf. 7.3). Como alternativa inferior, usar la implementación DoT nativa de Android para definir un servidor DNS recomendado (DoT) (cf. 7.3):

“Configuración” > “Internet y redes” > “DNS privado” > seleccionar “Nombre de host del proveedor de DNS privado” y entrar el servidor DNS deseado

- Si se debe absolutamente usar aplicaciones abusivas requiriendo permisos para funcionar, pasar temporalmente a un perfil de usuario secundario (o varios) en el afán de aislar totalmente sus actividades y estas aplicaciones del resto de sus datos:
“Configuración” > “Sistema” > “Varios usuarios” > “+ Agregar usuario”

### Android de origen

Las siguientes medidas son insuficientes para la privacidad dado que el SO es abusivo en sí, se recomienda usar una versión de Android modificada (cf. 5.1). Siendo dicho esto, para no estar perfilado de manera completa y continua con Android de origen:

- evitar todos los fabricantes chinos o Samsung y preferir una marca proponiendo “Android One” (es decir sin capa adicional del fabricante)
- nunca conectarse con una cuenta Google
- reemplazar las aplicaciones de origen (sobre todo el teclado) que pueden recolectar sus datos por las libres y respetuosas recomendadas en el punto 4
- desactivar todas las aplicaciones nefastas (Google, antivirus tercero, etc.) o no usadas y bloquear su acceso internet (desinstalarlas cuando es posible)

**GrapheneOS**

GrapheneOS integra nativamente un potente cortafuegos, directamente desde los ajustes de las aplicaciones, que permite bloquear totalmente el acceso internet de las aplicaciones deseadas. Aprovechenlo para desactivar el acceso internet de todas las aplicaciones que no lo requieren para funcionar:
“Configuración” > “Apps” > escoger una app > “Permisos” > “Network” > “Ver todas las apps que tienen este permiso”

Aprovechen también la función oferta unicamente por GrapheneOS y DivestOS para quitarles la autorización del acceso a los sensores (usado insidiosamente para la recolección de informaciones y el rastreo) a todas las aplicaciones comerciales o de código cerrado y también de las que no lo necesitan, por precaución:
“Configuración” > “Apps“ > escoger una app > “Permisos” > “Sensors” > “Ver todas las apps que tienen este permiso”

También es posible desactivar la atribución por defecto de este permiso a las nuevas aplicaciones instaladas (recordar atribuirla a las aplicaciones que la necesitan):
“Configuración” > “Privacidad“ > desactivar “Allow Sensors permission to apps by default”

GrapheneOS ofrece la posibilidad de recibir las notificaciones entre los perfiles de usuarios:
“Sistema” > “Varios usuarios” > “Send notifications to current user” (repetir la operación para cada perfil deseado)

GrapheneOS ofrece a pesar de todo la posibilidad de instalar los servicios Google sin privilegios, aislados en un perfil de usuario secundario en el afán de proporcionar una compatibilidad casi perfecta con las aplicaciones más abusivas que se niegan en funcionar sin estos últimos, tales como ciertas aplicaciones de bancos, por ejemplo. Para esto, abrir un perfil secundario (proceso detallado bajo las recomendaciones globales para Android y derivados) e instalar los servicios Google desde la aplicación “Apps” de GrapheneOS. Cuidado, las actividades vinculadas con las aplicaciones utilizadas con los servicios Google serán obviamente conocidas por este último.

Se recomienda altamente consultar la excelente y amplia documentación oficial de GrapheneOS en su sitio “https://grapheneos.org/faq”.

**CalyxOS**

CalyxOS integra nativamente un cortafuegos, la aplicación Datura, que les permite bloquear el acceso internet de las aplicaciones deseadas con un alto grado de control. Aprovechenlo para desactivar el acceso internet de todas las aplicaciones que no lo requieren para funcionar.

**iodéOS**

Por motivos de seguridad, se recomienda instalar y usar la tienda de aplicaciones libres Neo Store (cf. 4 y 9.2) en vez de F-Droid instalada por defecto. Se recomienda desinstalar este último.

De igual forma, el navegador por defecto de iodéOS, una versión modificada de Firefox recibiendo tardíamente las actualizaciones de seguridad y con una huella única, no debe ser utilizado. Instalen y usen, en su lugar, un navegador recomendado en el punto 4.

**/e/OS**

Cuidado, las cuentas “ecloud” no tienen cifrado de extremo a extremo (ZKE) y ya padecierón de una grave filtración de datos. Por lo tanto, se desaconseja encarecidamente hacer uso de una, por los menos con datos personales o importantes.

Por motivos de seguridad, se recomienda instalar y usar las tiendas de aplicaciones Neo Store (F-Droid) y Aurora Store (cf. 4 y 9.2) en lugar de la propia de /e/OS cuya implementación es imperfecta.

De igual forma, el navegador por defecto de /e/OS, una versión modificada de Bromite recibiendo tardíamente las actualizaciones de seguridad y con una huella única, no debe ser utilizado. Instalen y usen en su lugar un navegador recomendado en el punto 4.

## 9.2 Aplicaciones

### Neo Store (F-Droid) y Aurora Store

Estas tiendas de aplicaciones se deben descargar directamente desde sus páginas:
https://github.com/NeoApplications/Neo-Store/releases
https://auroraoss.com

Para poder instalarlas, otorgan el permiso de instalar aplicaciones desconocidas a su navegador cuando se lo solicite. Recuerden luego retirarlo por motivos de seguridad: “Configuración” Android > “Apps” > navegador utilizado > “Instalar apps desconocidas”

Recuerden no conectarse a Aurora Store con una cuenta Google personal. Usar en su lugar la cuenta anónima ofrecida.

Para poder encontrar e instalar algunas aplicaciones desde Neo Store, es necesario agregar sus propios repositorios. Para esto, ir a los ajustes de Neo Store (arriba a la derecha), luego bajo “repositorios” (simbolo abajo), añadir los repositorios “DivestOS Official”, “Guardian Project Official” y los otros deseados para aplicaciones tales como Bromite, Threema Libre, Molly (Signal), SimpleX Chat, NewPipe, Bitwarden o Collabora Office.

### Mull

Durante la instalación desde Neo Store, asegurarse de escoger la versión “DivestOS Official”, en vez de la versión F-Droid, en el afán de beneficiar lo antes posible de las actualizaciones y así mismo de los últimos parches de seguridad.
Mull ya viene en mayor parte configurado para la protección de la privacidad. Sin embargo, es necesario instalar la extensión uBlock Origin desde el menú y configurarla como explicado en el punto 9.5.

### NewPipe

Durante la instalación desde Neo Store, asegurarse de escoger la versión “NewPipe upstream repository”, en vez de la versión F-Droid, en el afán de recibir lo antes posible las actualizaciones corrigiendo los posibles fallos de funcionamiento por causa de modificaciones de Google en YouTube.

Para usar PeerTube con NewPipe: menú arriba a la izquierda > presionar “YouTube” > seleccionar “FramaTube”

**Telegram**

Ajustes:

- “Privacidad y seguridad” > “Seguridad” > activar “Verificación en dos pasos” para proteger su cuenta
- “Privacidad y seguridad” > “Chats secretos” > desactivar “Vista previa de enlaces” para evitar revelar a Telegram los enlaces compartidos en los chats secretos
- “Datos y almacenamiento” > desactivar todo bajo “Autodescarga de multimedia” para evitar descargar automáticamente malware en los canales o grupos públicos

Siempre usar los “chats secretos” (no disponibles para Telegram desktop) para que una conversación sea cifrada de extremo a extremo:

Perfil del contacto deseado > los tres puntos arriba a la derecha > “Iniciar chat secreto”

**RethinkDNS**

Activar un servidor DNS cifrado (DoH):

- “Configuración” Android > “Internet y redes” > “DNS privado” > seleccionar “Désactivado”
- abrir RethinkDNS > darle clic en “START” > seleccionar “DNS” arriba > seleccionar “Other DNS” > seleccionar el “+” abajo > entrar la dirección DoH de un servidor DNS recomendado (cf. 7.3) > darle clic en "ADD" > marcar en la lista la entrada recién añadida

Activar las listas negras locales para bloquear rastreadores, publicidad y más:

seleccionar “DNS” arriba > seleccionar “On-device blocklists” > darle clic en “Disabled” > confirmar “Download blocklists” > marcar las listas negras deseadas (preferiblemente todas las listas bajo “Security” y “Privacy”) > darle clic en “Apply”

**UntrackMe**

En el afán de redirigir o limpiar enlaces abusivos con UntrackMe, mantener presionado el enlace abusivo y seleccionar “compartir el enlace”. Después, escoger la aplicación UntrackMe, luego el navegador deseado y seleccionar “Siempre”.

## 9.3 Sistemas operativos para ordenadores

### Windows

Las siguientes recomendaciones son imperfectas y no garantizan la protección de datos, pues es recomendado usar una distribución de Linux (cf. 5.2) en vez de Windows. Siendo dicho esto, en el afán de no estar perfilado de manera completa y continua con Windows, seguir las siguientes recomendaciones:

- no usar ninguna versión anterior a Windows 10 pues son vulnerables/inseguras
- nunca conectarse con una cuenta Microsoft
- desactivar totalmente Cortana
- desactivar el historial de actividad
- ir en los ajustes, bajo “privacidad” y desactivar todo en cada una de las categorías a excepción de la autorizaciones necesarias para las aplicaciones usadas
- desinstalar (o cuando no es posible desactivar) Edge, Microsoft OneDrive, los antivirus (a excepción de Microsoft Defender) y todas las aplicaciones no usadas
- activar la dirección MAC aleatoria en los ajustes de la Wi-Fi
- preferiblemente usar otra sesión que la administradora para el uso a diario
- instalar el programa O&O ShutUp10++ para tener un mayor control sobre la privacidad
- instalar el programa Portmaster de safing.io para poder controlar (y bloquear) todas las conexiones entrantes y salientes con un alto grado de control (manualmente y con listas negras predefinidas para bloquear rastreadores y publicidad) y configurar un servidor DNS cifrado (cf. 7.3) para todo el sistema

### Linux (general)

Por motivos de seguridad, privilegien la instalación de programas Flatpak en vez de los tradicionales y configuren sus permisos gracias al programa Flatseal.

Configuración Wi-Fi con NetworkManager:
Clic derecho en el icono Wi-Fi, modificar las conexiones, seleccionar el Wi-Fi activo, bajo Wi-Fi seleccionar Dirección MAC clonada: Aleatoria.
Bajo ajustes IPv6, seleccionar Extensiones de confidencialidad IPv6: Activado (dirección temporal preferida).

### MX Linux

Advert Blocker (Bloquear-propaganda):
Seleccionar todas las opciones a excepción de “UNBLOCK” y luego confirmar.

## 9.4 Servicios y programas

### LibreWolf

LibreWolf ya está optimizado para la protección de la privacidad. Por lo tanto, no se recomienda cambiar sus ajustes “about:config”. Sin embargo, se recomienda activar el ajuste escondido “privacy.resistFingerprinting.letterboxing”, véase el punto 9.5 bajo “Configuración about:config” para poder activarlo.
Dado que se trata de una versión modificada de Firefox, por favor referirse a los puntos 6.1 y 9.5 para recomendaciones adicionales.

Cuidado, las versiones de LibreWolf para Windows y macOS no reciben automáticamente sus actualizaciones. Por lo tanto, es importante averiguar (aproximadamente una vez a la semana de preferencia) si una nueva versión está disponible en el sitio oficial, en el afán de beneficiar de los últimos parches de seguridad. Para actualizarlo, simplemente descargar y ejecutar el archivo de instalación disponible en el sitio.

### Portmaster

Cambiar el servidor DNS por defecto ya que Cloudflare es un actor centralizador y nefasto para la privacidad. En lugar de este último, es recomendado escoger una opción respetuosa propuesta en el punto 7.3 del documento, en función de sus preferencias y ubicación:
“Global Settings” a la izquierda > bajo “Secure DNS” > “Quick Settings” > seleccionar por ejemplo “AdGuard”

### Brave Search

Recuerden desactivar la telemetría activada por defecto:
Configuración: “Mostrar más” > “Estadísticas de uso anónimas”

### FreeTube

Es posible usar FreeTube con Invidious como proxy para limitar las conexiones a los servidores de Google. Sin embargo, la solución siguiente siendo imperfecta, se recomienda usar una instancia de Piped directamente desde el navegador.

Settings: - Player Settings : activar “Proxy Videos Through Invidious”
- Advanced Settings : entrar una instancia Invidious funcional

En caso de problema, cambiar de instancia Invidious.

## 9.5 Firefox y extensiones

### Configuración general

Para que Firefox respete y proteja la privacidad, es necesario configurarlo de manera adecuada. La configuración propuesta a continuación siendo relativamente protectora, es recomendado practicar la compartimentalización (cf. 6) para, entre otros, poder acceder a los sitios más recalcitrantes a la protección de la privacidad.
Los usuarios avanzados deseando una configuración aún mas restrictiva y entonces estando preparados para enfrentar más sitios que no cargan correctamente pueden, en vez de la configuración detallada a continuación, implementar la propuesta por el proyecto Arkenfox explicada en la pagina “https://github.com/arkenfox/user.js/wiki".

Perfiles:

Firefox ofrece la posibilidad de usar varios perfiles (configuraciones) diferentes al mismo tiempo. Se trata de una solución ideal para una transición rápida y simple desde una configuración restrictiva impidiendo una página web de cargar correctamente hacia una configuración más ligera, sin tener que cambiar de navegador. Todos los ajustes aportados, extensiones instaladas o marcadores añadidos serán guardados en el perfil en uso.
Para acceder a los diferentes perfiles de Firefox, entrar “about:profiles” en la barra de búsqueda. Esta página les permite crear nuevos perfiles y luego lanzarlos en una nueva ventana independiente, en cualquier momento, al darle clic en el botón “Launch profile in new browser” bajo el perfil deseado.

DNS over HTTPS:

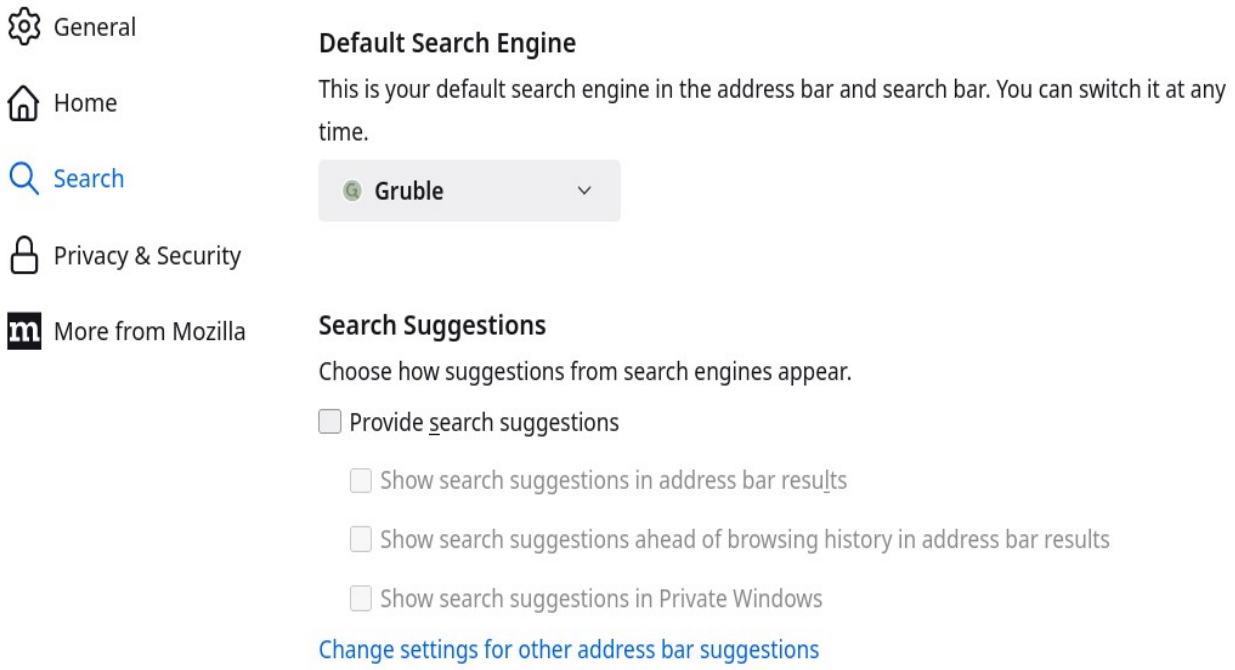
Se recomienda usar un servidor DNS respetuoso y cifrado a nivel global, mediante el programa Portmaster (cf. 9.4) por ejemplo, y entonces, desactivar la función "DNS over HTTPS" activada por defecto en Firefox para no sortear la configuración global. En el caso contrario, y si tampoco se usa un VPN, se recomienda dejar esta función activada. Ahora bien, es necesario cambiar el servidor DNS por defecto ya que Cloudflare es un actor centralizador y nefasto para la privacidad. En lugar de este último, es recomendado escoger una opción respetuosa propuesta en el punto 7.3 del documento, en función de sus preferencias y ubicación.

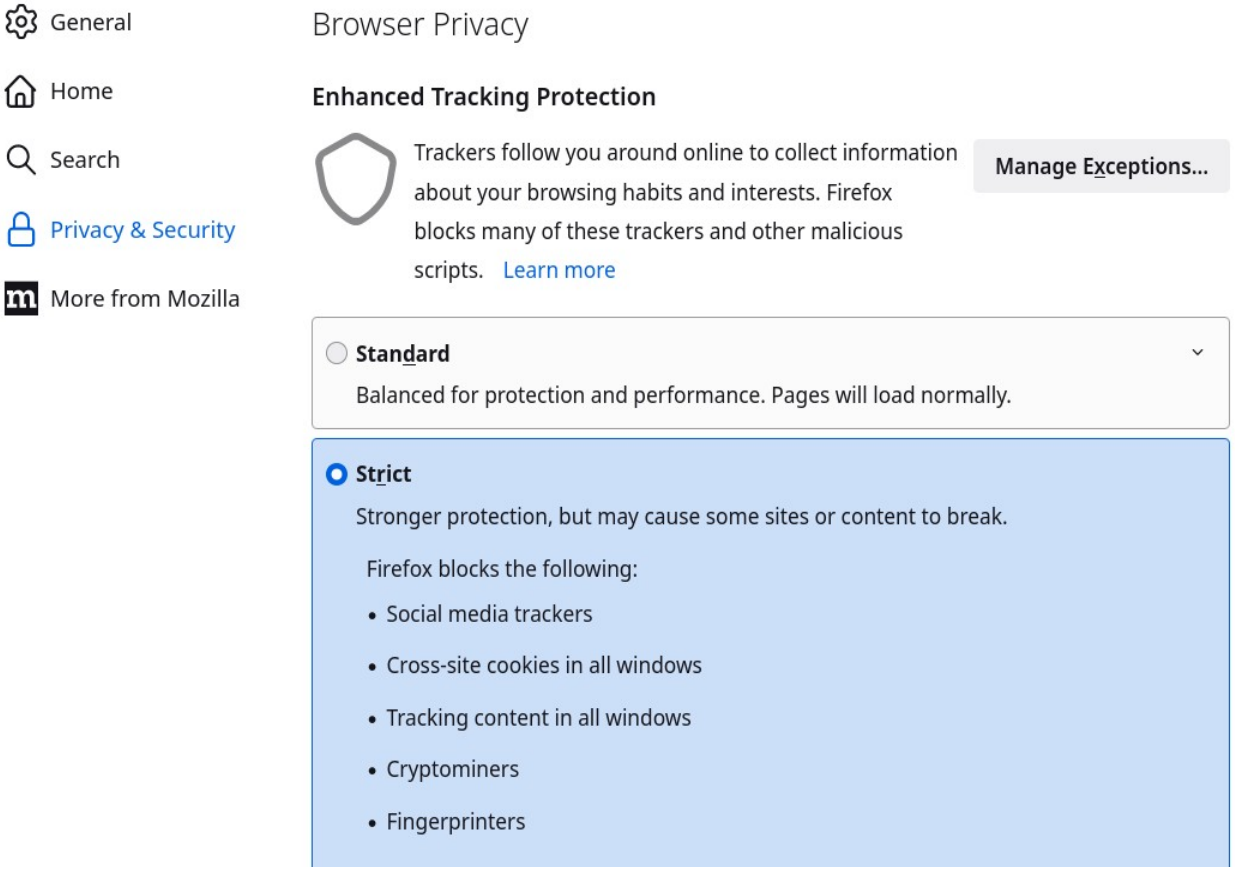
Para esto: “General” > todo abajo “Network Settings” > “Enable DNS over HTTPS” > bajo “Use Provider” seleccionar “Custom” > entrar la URL del servidor DoH deseado.

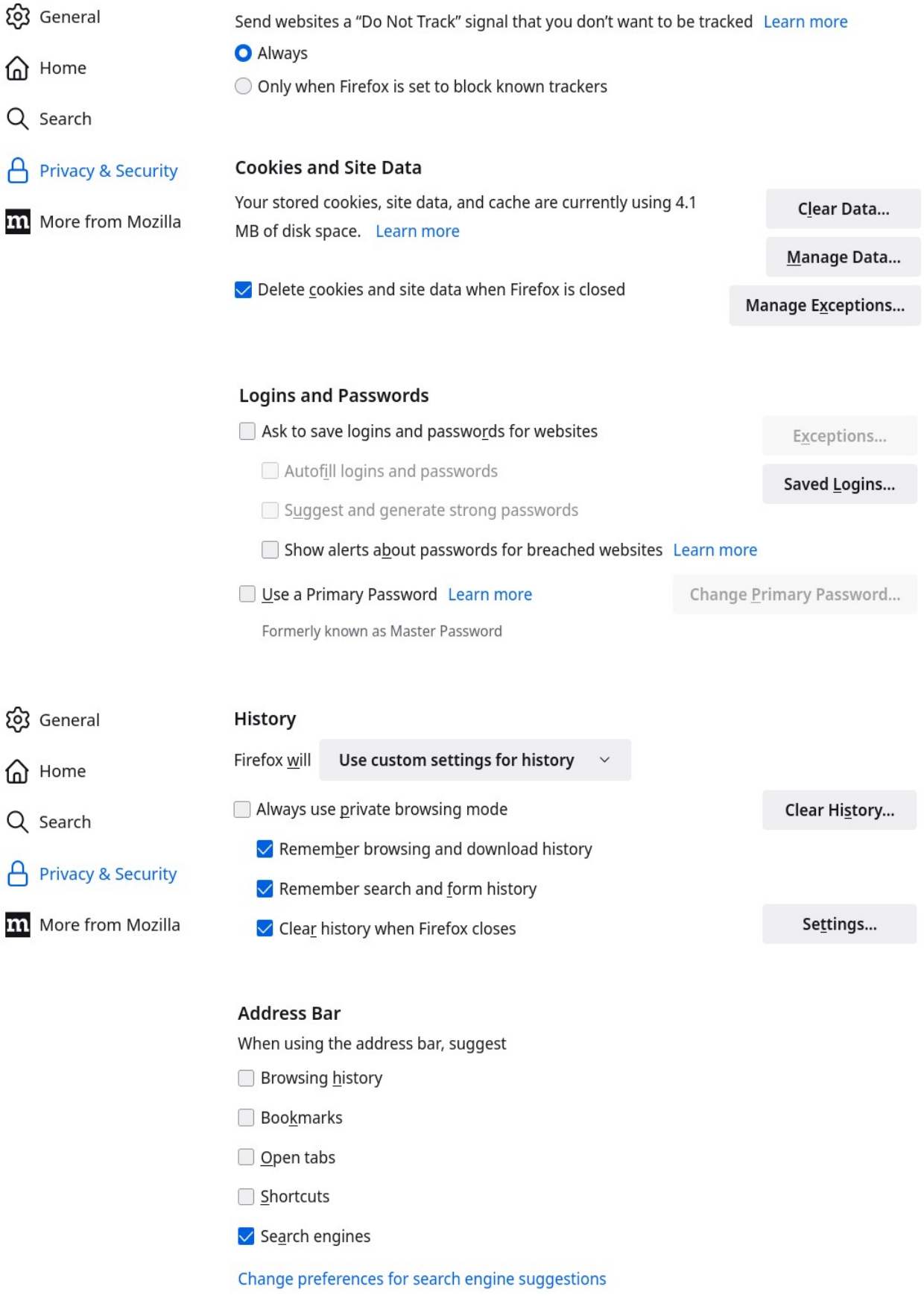
Buscadores:

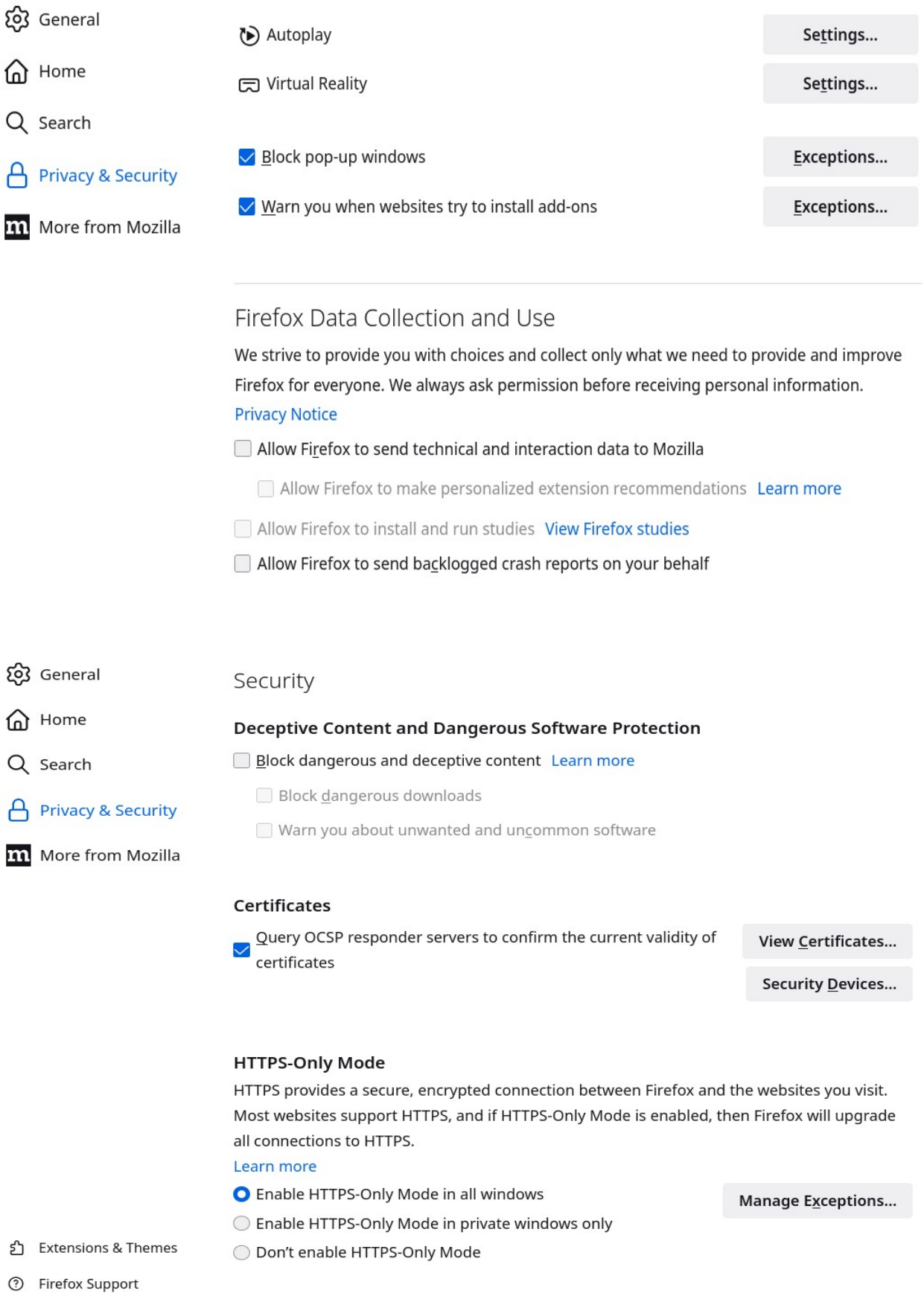
Para agregar un buscador adicional, tal como Brave Search o una instancia de searXNG, en Firefox o LibreWolf, simplemente entrar en la pagina web del buscador deseado y realizar clic derecho en la barra de direcciones y luego seleccionar la opción para agregar el buscador deseado.

A continuación, el resto de la configuración general recomendada en imágenes:




General
Home
Search
Privacy & Security
More from Mozilla
Send websites a "Do Not Track" signal that you don't want to be tracked Learn more
Always
Only when Firefox is set to block known trackers
Cookies and Site Data
Your stored cookies, site data, and cache are currently using 4.1 MB of disk space. Learn more
Clear Data...
Manage Data...
Delete cookies and site data when Firefox is closed
Manage Exceptions...
Logins and Passwords
Ask to save logins and passwords for websites
Exceptions...
Autofill logins and passwords
Saved Logins...
Suggest and generate strong passwords
Show alerts about passwords for breached websites Learn more
Use a Primary Password Learn more
Change Primary Password...
Formerly known as Master Password
General
Home
Search
Privacy & Security
More from Mozilla
History
Firefox will
Use custom settings for history
Always use private browsing mode
Clear History...
Remember browsing and download history
Remember search and form history
Clear history when Firefox closes
Settings...
Address Bar
When using the address bar, suggest
Browsing history
Bookmarks
Open tabs
Shortcuts
Search engines
Change preferences for search engine suggestions


General
Home
Search
Privacy & Security
More from Mozilla
Autoplay
Settings...
Virtual Reality
Settings...
Block pop-up windows
Exceptions...
Warn you when websites try to install add-ons
Exceptions...
Firefox Data Collection and Use
We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.
Privacy Notice
Allow Firefox to send technical and interaction data to Mozilla
Allow Firefox to make personalized extension recommendations Learn more
Allow Firefox to install and run studies View Firefox studies
Allow Firefox to send backlogged crash reports on your behalf
General
Home
Search
Privacy & Security
More from Mozilla
Security
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content Learn more
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
HTTPS-Only Mode
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.
Learn more
Enable HTTPS-Only Mode in all windows
Enable HTTPS-Only Mode in private windows only
Don't enable HTTPS-Only Mode
Manage Exceptions...
Extensions & Themes
Firefox Support

**Configuración de las extensiones**

Es importante autorizar las extensiones siguientes a funcionar en navegación privada y activar sus actualizaciones automáticas.

uBlock Origin:

- Settings: activar “I am an advanced user” y activar todo bajo “Privacy”

- Filter Lists: activar TODAS las listas, excepto bajo “Regions” (solo activar para los idiomas usados)
Las listas bajo “Annoyances” y “Multipurpose” pueden impedir el funcionamiento de redes sociales abusivas

- Agregar las listas siguientes desde filterlists.com: “Actually Legitimate URL Shortener Tool” (reemplaza ClearURLs), “Energized Ultimate Protection”, “Energized IP Extension”, “Energized Social Extension”, (“Energized Xtreme Extension”)
Para agregar una lista desde filterlists.com: dar clic en el botón de la lista a la izquierda > dar clic en "Subscribe" en el menú habiendo aparecido

- Seguir el tutorial de la página web siguiente para establecer las reglas de filtración dinámica (opcional pero recomendado):
https://www.maketecheasier.com/ultimate-ublock-origin-superusers-guide

LocalCDN:

En los ajustes ir bajo “Advanced” > bajo “Generate rule sets for your adblocker” seleccionar uBlock > copiar el conjunto de reglas dadas > abrir la extensión uBlock Origin > en sus ajustes ir bajo “My rules” > pegar en la parte derecha el conjunto de reglas copiadas > dar clic en “Save” > dar clic en “Commit”.

LibRedirect:

Settings: - “YouTube” > “Frontend” escoger “Piped” > bajo “Default Instances” solo activar “https://piped.projectsegfau.lt” y “https://piped.adminforge.de”

- activar o desactivar las otras plataformas e instancias deseadas (cf. 7.)

**Configuraciones about:config**

Acceder a estos ajustes entrando “about:config” en la barra de direcciones de Firefox. Esas diversas configuraciones mejoran la privacidad y la seguridad del navegador. Los elementos entre paréntesis no suelen ser deseables en todos los casos.

accessibility.force_disabled = 1

beacon.enabled = false

browser.formfill.enable = false

browser.sessionstore.interval = 60000

browser.sessionstore.privacy_level = 2

browser.urlbar.speculativeConnect.enabled = false

browser.urlbar.trimURLs = false

browser.xul.error_pages.expert_bad_cert = true

captivedetect.canonicalURL = borrar

(dom.push.enabled = false)

dom.serviceWorkers.enabled= false

geo.provider.ms-windows-location = false

geo.provider.network.url = reemplazar dirección por :

https://location.services.mozilla.com/v1/geolocate?key=%MOZILLA_API_KEY%

geo.provider.use_corelocation = false

geo.provider.use_geoclue = false

geo.provider.use_gpsd = false

google = borrar las direcciones

intl.accept_languages = en-US, en

javascript.use_us_english_locale = true

Entrar manualmente este parámetro en la barra de búsqueda para poder activarlo

media.peerconnection.ice.default_address_only = true

media.peerconnection.ice.no_host = true

media.peerconnection.ice.proxy_only_if_behind_proxy = true

network.captive-portal-service.enabled = false

network.dns.disableIPv6 = true

network.dns.disablePrefetch = true

network.IDN_show_punycode = true

(network.http.referer.XOriginPolicy = 2)

network.http.referer.XOriginTrimmingPolicy = 2

network.http.speculative-parallel-limit = 0

network.prefetch-next = false

normandy = false para todos los elementos + borrar las direcciones e identificadores

pdfjs.enableScripting = false

places.history.enabled = false

pocket = false para todos los elementos + borrar las direcciones e identificadores

privacy.clearOnShutdown.offlineApps = true

privacy.query_stripping.enabled.pbmode = true

privacy.resistFingerprinting = true

privacy.resistFingerprinting.letterboxing = true

Entrar manualmente este parámetro en la barra de búsqueda para poder activarlo

report (reporter/reporting) = false para todos los elementos + borrar las direcciones

safebrowsing = false para todos los elementos + borrar direcciones e identificadores

security.cert_pinning.enforcement_level = 2

(security.mixed_content.upgrade_display_content = true)

security.OCSP.require = true

(security.ssl.enable_false_start = false)

security.ssl.require_safe_negotiation = true

security.tls.enable_0rtt_data = false

telemetry = false para todos los elementos + borrar las direcciones e identificadores

webgl.disabled = true