GROG&TOR

RECURSERO DE AUTODEFENSA DIGITAL

UTOPIA PIRATA

Partido Interdimensional Pirata

GROG & TOR

RECURSERO DE AUTODEFENSA DIGITAL

partido
interdimensional
pirata

FUNDACIÓN
ROSA
LUXEMBURGO

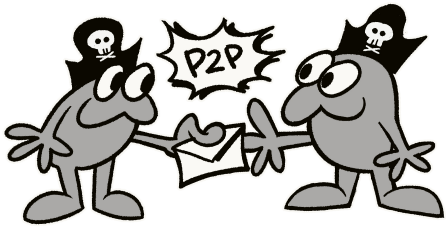
“Esta publicación fue realizada con el apoyo de la Fundación Rosa Luxemburgo (FRL) y fondos del Ministerio Federal de Cooperación Económica y Desarrollo de Alemania (BMZ). Las opiniones expresadas en ella no reflejan necesariamente los puntos de vista de la FRL”.

Septiembre de 2026.

Contacto: contacto@partidopirata.com.ar

Indice

¿Qué es el PIP?



Somos un colectivo de personas y cyborgs que nos organizamos en base a relaciones de afinidad, solidaridad, cuidados mutuos y afectividad.

Esto no significa que tengamos que estar de acuerdo en todo ni que pretendamos homogeneizarnos en algún “estilo pirata”. Significa, sobre todo, que desechamos las lógicas instrumentalistas y productivistas. Por sobre “los fines” o “los productos” de ciertas acciones u objetivos políticos preferimos ejercitar otras lógicas: de autocuidados, procesuales, de acompañamiento y de relacionamiento.

Les piratas nos damos unos acuerdos básicos de cuidados mutuos a través de nuestros códigos para compartir, que nos guían en la convivencia cotidiana y en el reconocimiento mutuo. Nos organizamos en torno a barcas y son grupos de afinidad sobre temas específicos relacionados con nuestros activismos. Las barcas se comunican entre sí y colaboran en distintas acciones.

Como colectivo practicamos: Talleres de autodefensa digital, Comunicación alternativa, comunitaria, popular. Autodeterminación & #HacerloNosotrasMismas. Prácticas de cuidados mutuos y colectivos. Editoriales libres, independientes y autogestivas. Emancipación tecnológica y cognitiva. Y quizás también archivismo y piratería :)

Si quieren sumarse al PIP pueden revisar nuestra publicación *¡Quiero ser pirata!*

¿Qué son las Grog&Tor?

Usamos este término para referirnos a eventos presenciales realizados en diferentes espacios y con diferentes públicos que buscan expandir saberes sobre privacidad y seguridad en internet.

El nombre combina dos mundos: "Grog", en referencia a la icónica bebida del videojuego Monkey Island (símbolo de la aventura y camaradería pirata), y "Tor", por la red de anonimato (símbolo de la protección y libertad digital).

Nos interesa construir comunidades con quienes asisten donde futuras dudas e inquietudes puedan ser resueltas entre les participantes y las piratas que estuvieron en el encuentro.

Además, mantenemos un Recursero Digital con información sobre riesgos de privacidad y seguridad, así como las técnicas que exploramos y recomendamos.

Éste se encuentra en: **https://partidopirata.com.ar/recursero-gt/**

Este texto es un resumen en base a este Recursero digital, realizado en agosto 2026. Recomendamos chequear nuestra versión online, que además de estar mas explayado, cuenta con posibles actualizaciones de información.

Acá vas a encontrar información sobre autodefensa digital, herramientas recomendadas y buenas prácticas para proteger tu privacidad y seguridad en internet. No es un manual de uso, ni una guía completa, sino información que esperamos pueda ser de utilidad para empezar a pensar en tu autodefensa digital.

Recursero G&T

Espera... ¿Qué es la autodefensa digital?

La autodefensa digital es el conjunto de hábitos y herramientas que usamos para proteger nuestra información personal en internet y a nuestros dispositivos de amenazas como virus, robos de datos o accesos no autorizados. Es como cerrar tu casa con llave: cuidas tus contraseñas, no caes en estafas, usas conexiones seguras y controlas quién ve tus datos.

“Pero yo no tengo nada que ocultar, no me importa que me vigilen“

Ante nuestras charlas, mucha gente se pregunta: ¿Por qué me debería importar que me vigilen? Pero la vigilancia no sirve solo para detectar criminales o terroristas (la excusa predilecta). A partir de estos datos los monopolios de tecnología y los estados pueden:

• Regular los discursos que circulan en la población y posicionar mejor los mas convenientes.

• Decidir a quién entregarle un crédito, una cobertura médica, un trabajo o una libertad condicional de forma algorítmica o basada en información privada.

• Establecer los precios de productos y servicios de manera dinámica, de forma que te saquen lo más que puedan.

• Censura y persecución de disidentes políticos.

• Aislamiento de individuos: creación de nichos que funcionan como una cámara de eco e invisibilizan otras realidades.

Queremos que el modelo de negocios no sea enfermarnos para generar el mayor nivel de capital posible, si no que lo que utilizamos tenga en cuenta nuestro bienestar y disfrute como un bien necesario y suficiente.

Modelado de Amenazas

No existe la seguridad infalible, por eso nos conviene adaptar las medidas que tomemos en cada caso a nuestras necesidades particulares. No serán iguales las medidas que necesite tomar una periodista para comunicarse con una fuente, que para une amigue mensajeando a otre sobre la noche anterior o un abogado hablando con su cliente.

Al proceso de entender las necesidades y prioridades de seguridad lo llamamos Modelado de Amenazas. Las siguientes preguntas sirven para ir orientándonos en cuánto a nuestras acciones:

• **¿Qué queremos proteger?** Por ejemplo: mis contactos de seres queridos / facultad / militancia, mis cuentas bancarias, la privacidad de mis fotos, mi ubicación.

• ¿De quién quiero protegerlo? Por ejemplo: no quiero que el Estado sepa a qué marcha voy, no quiero que alguien le haga phishing a mi familia haciéndose pasar por mí.

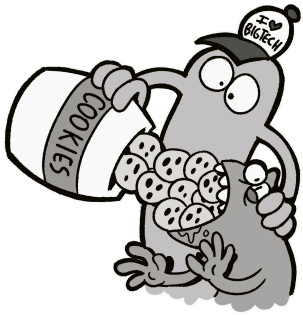
• **¿Qué tan probable es que tenga que protegerla?** Por ejemplo: si mi preocupación es que el Estado vea a quién llamé, las empresas telefónicas tienen completo acceso a esa información y es accesible vía una orden judicial.

¿Cuáles son las consecuencias si fallo en protegerlos? Por ejemplo: me vacían la cuenta del banco, pero dependiendo del método que usen puedo desconocer esos gastos y que el banco me lo devuelva.

La privacidad como espacio de libertad y soberanía

Más allá de la defensa pasiva contra la vigilancia, proteger nuestros datos nos permite recuperar la soberanía sobre nuestra vida digital.

Cuando los datos no son una mercancía extraída de nosotros, la tecnología deja de ser una herramienta de control y se convierte en un medio de expresión y conexión genuina.



• **Autonomía en las decisiones:** Al no estar bajo el escrutinio constante de algoritmos de perfilado, podemos navegar, aprender y crear sin que nuestras acciones sean condicionadas por recomendaciones diseñadas para maximizar el consumo o moldear nuestro pensamiento.

• **Seguridad para la disidencia:** Un espacio privado es el único lugar donde se puede experimentar, debatir y organizar sin el miedo a la represalia, censura o al aislamiento social.

• ***Conexión humana genuina:*** Al reducir el ruido del marketing invasivo y el trackeo, logramos interacciones digitales más directas y significativas, centradas en el intercambio de ideas y no en la extracción de valor.

• **La salud mental se protege:** Menos interrupciones publicitarias y menos ansiedad generada por comparaciones artificiales (bombardeadas por algoritmos) significa un uso de la tecnología más consciente y menos adictivo.

Todas las Herramientas que recomendamos son Software Libre… ¿por qué?

El Software libre son programas cuyo código está publicado, que cualquiera puede colaborar si respeta los códigos de aquella comunidad, y que tienen licencias que autorizan que se comparta y se hagan otras variantes del software. Nos parece importante usar Software Libre en lo posible porque:

• **Es auditable:** como el código es públicamente accesible, hay una comunidad de desarrolladores a quienes le importan la privacidad y seguridad que revisan que los programas efectivamente hagan lo que prometen hacer, y que no incluyan características no deseadas tales como publicidad, trackeo o espionaje.

• **Es adaptable:** al poderse realizar distintas versiones, los programas se pueden adaptar a las necesidades de distintas comunidades, traducir a distintos idiomas, hacer accesible a ciegxs, agregarles funcionalidades especificas, etc.

• **No es arancelado:** la plata no es un obstáculo para usarlo, pero hay formas de colaborar (monetariamente y no) con lxs desarrolladorxs.

• **Se aprende:** existen espacios de discusión y formación sobre las distintas herramientas y aprendemos a recuperar control sobre la tecnología. :)

• **No hay una empresa cambiándote los términos de uso todo el tiempo:** Las licencias libres garantizan que el software hará lo que dice hacer hoy y mañana, sin que una corporación decida maliciosamente de un día para el otro que tu privacidad vale menos que sus ganancias.

• **Evita la obsolescencia programada:** muchos Softwares Privativos, como windows, agregan características que exigen una computadora más nueva generando “residuos electrónicos” que son considerados obsoletos. Esto además impacta en el bolsillo de lxs trabajadores y les deja sin acceso

a software actualizado, generando sistemas vulnerables masivos. En cambio, dentro de las comunidades de Software Libre, hay muchas personas comprometidas a optimizar los programas, como las comunidades alrededor de GNU/Linux y LibreOffice o Inkscape que son programas FOSS.

¿Qué usas en la computadora y para qué?

Es momento de hacer un inventario. ¿Usás Microsoft Office para escribir documentos? ¿Usás Chrome para navegar? ¿Usás Windows solo porque "ya venía"?

Preguntémonos: ¿podríamos hacer lo mismo con software libre? ¿El software privativo que usamos, nos deja hacer todo lo que queremos o posee limitaciones?¿Y estas limitaciones son reales o fueron impuestas para beneficio de otrxs por sobre nuestra necesidad?
Entonces: ¿Nuestras herramientas nos pertenecen o nosotres le pertenecemos a ellas?

Hoy, una persona usuaria de Windows 11 no puede empezar a usar su propia computadora sin una cuenta @microsoft. Está forzada a tener instalada la IA de Copilot. No puede quitar del incio la integración forzada de Bing, que hace que cualquier error en una búsqueda termine abriendo el navegador con resultados innecesarios. Y cada actualización obligatoria de Windows 11 le traerá posibles mejoras pero también cambios que eliminen funciones esenciales o añadan otras que no quiera. Microsoft se ocupara más en anclarle a sus propios servicios que en mejorar su experiencia como usuarie sin importarle que ya halla pagado por su producto. Y todo esto es sin contar el rastreo constante, la telemetría que envía datos de uso de nuestros dispositivos hacia Microsoft o el espacio publicitario en el menu de inicio.

Al migrar a alternativas como LibreOffice, Firefox o un sistema operativo Linux, no solo recuperamos la privacidad, también liberamos recursos de nuestra computadora que antes estaban dedicados a "llamar a la casa" de sus amos.

Si queres empezar a usar software libre, podés encontrar alternativas a los programas que usás en https://alternativeto.net/

Mensajería

Activar números

Para algunas apps vas a necesitar tener una **linea de teléfono**. Si no querés que te puedan rastrear de esa manera, vas a tener que averiguar cómo conseguir una línea que no esté a tu nombre. ¿Existe forma de hacer eso? Capaz que si. ¿La vamos a decir públicamente? Capaz que no.

Apps de mensajería

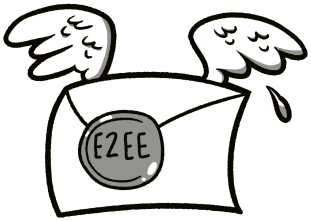
Las míticas preguntas: **¿WhatsApp es seguro? ¿Es mejor Telegram?** Para responder tendríamos que entender a qué nos referimos cuando decimos mejor:

En el mundo digital, "mejor" puede significar por ejemplo: ¿Cuánto control tengo sobre mis datos? ¿Quién tiene acceso a ellos? ¿Puedo verificar si la app realmente hace lo que dice?

No recomendamos usar WhatsApp aunque posea cifrado de extremo a extremo en sus chats, ya que recopila gran cantidad de metadatos a disposición de Meta[1]. Esto le permite establecer patrones de uso que, aunque no revelen tus conversaciones, describen con bastante precisión tu comportamiento digital. Además posee **código cerrado**, por lo que no se puede saber realmente si cumplen con sus promesas de privacidad.

¿Qué alternativas tenemos?

Signal: Está cifrada extremo a extremo, es de código mayormente abierto y está enfocada en privacidad y seguridad. No recopila datos personales, pero requiere de un número de teléfono para registrarse. Si buscás una opción aún más transparente, existe Molly, un fork de Signal que es código abierto en su totalidad. Tenemos un tutorial de como instalarlo ;)
https://partidopirata.com.ar/fdroid-gt/



XMPP: Es un protocolo de mensajería descentralizado. Como tal, no depende de un ente único, sino que hay múltiples implementaciones en servidores autónomos de todo el mundo. Generalmente no requiere número de teléfono ni dirección de email para registrarse y soporta cifrado extremo a extremo. Recomendamos mantenerse con las apps y proveedores más populares para evitar problemas de compatibilidad (Por ej. Prav, Conversations, Gajim). Más info: https://joinjabber.org

Telegram: No recomendamos Telegram como alternativa porque no posee cifrado de extremo a extremo por default, solamente se puede utilizar en chats privados en smartphones. Lo positivo que tenia Telegram es que no entregaba información a los estados. En 2024, luego de la detención de Pável Durov (el dueño de la plataforma) actualizó sus políticas pudiendo llegar a compartir el número de registro y la dirección IP ante solicitudes estatales. Se pueden consultar las usuarias afectadas por esto a través de unx bot: https://t.me/transparency.

Podés revisar más opciones y sus características en: https://liberaturadio.org/recursos-y-plataformas-libres/

Recordemos también la importancia de los mensajes temporales, para que ningún mensaje con tonos sospechosos sea leído por ojos sin humor ;)

Tips para usar Whatsapp de forma más segura

Recomendamos activar la **"Verificación en dos pasos"**. Esto nos permitirá crear un PIN (clave numérica de 6 dígitos) la cual será solicitada al momento de trasladar la cuenta a otro dispositivo (por ej: si el nuestro se rompiese o fuese robado).

Esto nos protegerá de intentos de robo de cuenta, ataques cada vez mas frecuentes hoy en día. Para hacerlo, debemos tocar los 3 puntitos de la esquina superior derecha > Ajustes > Cuenta > Verificación en dos pasos.

En caso de que no lo hayamos activado y nuestra cuenta haya sido robada:

• Advertir lo sucedido a contactos, ya que el atacante usará nuestro número para estafar haciéndose pasar por nosotres.

• Contactar al soporte de Whatsapp en https://wa.me/support

• En el cuerpo del mensaje, indicar que nos han robado la cuenta y contar brevemente lo sucedido. Por ejemplo: "Recibí un mensaje/llamada haciéndose pasar por Fulanito o por una institución, donde me pidieron un código que recibiría por SMS..." o "De un momento al otro, mi cuenta se cerró y mis familiares me dijeron que alguien les pedía dinero haciéndose pasar por mí...".

• Indicar nuestro número de teléfono asociado a la cuenta con todo su prefijo (ejemplo en CABA: +54 9 11 xxxx xxxx).

• En un lapso de entre 2 y 7 días hábiles, aunque WhatsApp no suele responder, deberíamos poder volver a acceder a nuestra cuenta.

Sobre las copias de seguridad (Backups)

Recomendamos desactivar la copia de seguridad en Google Drive, ya que por defecto guarda nuestros chats sin cifrar, quedando al alcance de Google, autoridades y demás atacantes.

• Si querés conservar conversaciones importantes, recomendamos que las descargues localmente en texto plano. Entendamos que estas permanecerán sin cifrar dentro de nuestro dispositivo, por lo que será nuestra responsabilidad brindarles seguridad (podemos optar por cifrarlas nosotres mismos y/o moverlas a otro dispositivo más seguro).

• Si a pesar de todo preferís el backup automático en Google Drive, te sugerimos al menos activar la opción de "Copia de seguridad cifrada de extremo a extremo".

Correo electrónico

El capitalismo de vigilancia se basa en la recolección masiva de datos y los principales proveedores de correo electrónico (como Gmail y Outlook) están atravesados por esta lógica. En pos de recuperar el control sobre nuestros datos y hacer valer nuestra privacidad, recomendamos las siguientes alternativas:

• ***Proton:*** Ofrece una casilla de email gratuita de 1 GB de almacenamiento, con opciones de pago para mayor almacenamiento y otras funcionalidades. No requiere brindar información personal de ningún tipo, ni número de teléfono, ni correo electrónico. Ofrecen correo electrónico cifrado de extremo a extremo por defecto para destinatarios que también usen Protonmail. Y existe una serie de pasos a seguir para obtener cifrado con externos. https://proton.me/es-es/mail

• **Riseup:** Ofrece una casilla de email gratuita con 1GB de almacenamiento. Para registrarse es necesario que alguien que ya tenga una cuenta te envíe un código de invitación. No requiere brindar información personal de ningún tipo, ni número de teléfono, ni correo electrónico. Riseup encriptará los correos siempre que sea posible (es decir, siempre que

quien reciba el mail utilice un proveedor compatible). Los correos enviados desde una casilla de Riseup no revelarán tu IP. No registran tu dirección de IP al utilizar sus servicios. https://riseup.net/es/email https://riseup.net/es/email/settings/mail-accounts

• **Disroot:** Desarrollan y distribuyen una gran cantidad de herramientas digitales tales como correo electrónico, almacenamiento en la nube, documentos compartidos, mensajería instantánea descentralizada, búsquedas anónimas en la web, videollamadas, etc. Ofrecen una casilla de email gratuita con 2GB de almacenamiento. Para registrarse únicamente requieren una dirección de email (puede utilizarse un email descartable) y tarda 48hs en procesar la solicitud y habilitar la cuenta. Ofrecen cifrado TLS (cliente-servidor) por defecto, y fomentan el uso de cifrado extremo a extremo. https://disroot.org/es/services/email

Correos electrónicos descartables

En distintas situaciones, principalmente si deseamos registrarnos en un sitio manteniendo nuestro anonimato, podría sernos útil emplear casillas de **correo temporales**. A diferencia de tu buzón principal, estas cuentas son efímeras y diseñadas para desaparecer. Permiten mantener el anonimato ante sitios que bloquean el acceso sin cuentas, y evitan que nuestros datos queden vinculados a servicios de los que no queremos dejar rastro ni necesitaremos recuperar en el futuro.

Algunos sitios que brindan este servicio:

https://temp-mail.org https://10minutemail.com

https://www.guerrillamail.com https://www.yopmail.com

Sin embargo, debido a la naturaleza temporal de estos mails, no deberían ser utilizados para reemplazar un mail principal sino para complementarlo.

Buscadores

Un buscador es el motor que procesa tu consulta. Cuando escribís "receta de pizza" en Google, Google sabe qué buscas, cuándo, desde qué dispositivo y qué otros términos has buscado antes. Esto para nosotras es un problema de privacidad ya que esta información es guardada y puede ser relacionada a nuestra identidad y utilizada tanto por las empresas para mostrar publicidad, como por agencias guvernamentales que les compran esa información.

Para proteger nuestra privacidad, podemos optar por alternativas que priorizan el anonimato y no nos rastrean:

• **DuckDuckGo:** No guarda historial de búsquedas ni crea perfiles de usuario. Además, ofrece herramientas adicionales como el cifrado de formularios y la protección contra rastreadores en el navegador.

• **Brave Search:** Brave construye su índice propio desde cero, lo que significa que no depende de otros motores de búsqueda para obtener resultados. No guarda historial, no crea perfiles de usuario y no comparte datos con terceros.

• **Startpage:** Actúa como un intermediario: envía tu consulta a google, pero elimina los datos de identificación antes de procesarla.

• **SearXNG:** SearXNG es un metabuscador que agrega resultados de múltiples motores (Google, Bing, Wikipedia, etc.) y los mezcla para ofrecer resultados neutros y sin publicidad. Al ser autoalojable, podés usar instancias públicas verificadas o instalar tu propia instancia local para un control total sobre tus consultas.
Directorio de instancias confiables: searx.space

Navegadores

El navegador es la puerta de entrada a internet; si no nos puede proveer suficiente privacidad, todo lo demás para lo que lo utilicemos tampoco podrá hacerlo.

Se pueden visitar sitios como BrowserLeaks.com o Analytical.io para ver qué información filtran nuestros navegadores.

Podemos recomendar:

• **Firefox:** Es de código abierto y permite configurar ajustes de privacidad avanzados (como el bloqueo de rastreadores). Es ideal para el uso diario si se configura correctamente (hay que desactivarle la IA!)
https://www.mozilla.org/es-AR/firefox/all/desktop-release/

• **LibreWolf:** Basado en Firefox, pero con la telemetría y servicios de Google eliminados de fábrica. Es una excelente opción para usuarios que quieren privacidad por defecto sin tener que configurar manualmente cada ajuste.
https://librewolf.net/

• **Tor Browser:** El estándar de oro para el anonimato. Enruta tu tráfico a través de la red Tor, ocultando tu dirección IP y dificultando el rastreo por parte de terceros. Ideal para situaciones de alto riesgo o acceso a contenidos restringidos.
https://www.torproject.org/es/download/

• **Mullvad Browser:** Es esencialmente el navegador Tor, pero diseñado para funcionar también fuera de la red Tor. Ofrece las mismas características de privacidad que Tor pero con una interfaz más ligera y fácil de usar para el día a día.
https://mullvad.net/browser

Bloqueadores de anuncios

Un bloqueador de anuncios es una extensión para nuestro navegador que impide que la mayoría de anuncios se carguen y muestren en las páginas que visitamos. Funcionan utilizando listas que contienen las direcciones de servidores donde están los anuncios. Si desde la página se intenta acceder a una de esas direcciones, nuestro bloqueador lo impide. Además de evitar ver anuncios, los bloqueadores nos proveen mucha más privacidad, seguridad y velocidad

• **Privacidad:** La mayoría de anuncios llevan asociadas cookies de rastreo (tracking cookies) que registran nuestra actividad en los sitios que visitamos. Al frenar gran parte de este espionaje digital, ya que no permitir mostrar anuncios también deshabilita las cookies de rastreo, los bloqueadores de anuncios son una de las formas mas fáciles de aumentar muchísimo nuestra privacidad online.

• **Seguridad:** El malvertising es una técnica por la que ciberdelincuentes insertan código malicioso en anuncios legítimos. Entonces puede pasar que entramos a una web de confianza pero junto a esta se cargan anuncios que pueden infectar tu dispositivo sin que apretes nada. Un buen bloqueador corta de raíz esta vía de ataque.

• **Velocidad:** Los anuncios, especialmente los vídeos y los interactivos, son de los elementos más pesados de una página web. Bloquearlos no solo limpia la pantalla, sino que puede hacer que las páginas carguen entre un 20% y un 40% más rápido. Si navegas con datos móviles, ahorras tiempo y guita.

Bloqueadores recomendados

• **uBlock Origin:** Es ligero, rápido y consume muy pocos recursos de tu navegador.
https://github.com/gorhill/ublock

• **AdGuard:** Tiene una interfaz muy amigable y permite personalizar qué se bloquea y qué no con mucha facilidad.
https://adguard.com/es es la url de Adguard.

• **AdNauseam:** Aparte de no mostrar los anuncios, envía clicks a escondidas a todos los anuncios que hubieramos visto. Esto ofusca nuestro perfil y le de una pequeña ganancia a los sitios que visitamos, la cual pagan los proveedores de anuncios sin que tengamos que verlos.
https://adnauseam.io/

También hay navegadores que ofrecen bloqueadores de anuncios incorporados, como por ejemplo Brave.

¡A tener en cuenta!

Algunos sitios pueden detectar que estamos usando un bloqueador y impedir el acceso a su contenido hasta no deshabilitar el bloqueador.

Todos los bloqueadores de anuncios tienen la opción de deshabilitarse momentáneamente o para algunos sitios en particular, entonces solo es cuestión de tener esto en cuenta y saber dónde aparece esa opción para el bloqueador de anuncio que nos instalamos. Por otro lado suelen no funcionar en ventanas de incognito por defecto, por lo que abrir la pagina en una de estas puede ser otra opción.

Recordá que los anuncios son la fuente de ingresos de muchos sitios pequeños, por lo que podemos tener la practica pausarlos en páginas que nos interese apoyar de esta forma o usar AdNauseam.

Sistemas Operativos

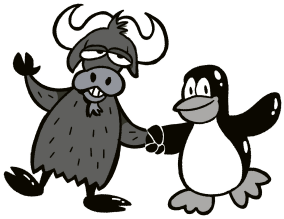
Recomendamos para temas de seguridad utilizar sistemas operativos distintos a Windows y MacOS

GNU/Linux es uno de los sistemas operativos más populares y versátiles. Sin embargo, dentro lo que es Linux, existen muchisimas **distribuciones** o distros y esto puede generar confusión entre lxs usuaries menos familiarizados con el tema.

Las distribuciones de Linux son variantes del sistema operativo Linux que suelen estar diseñadas para satisfacer necesidades específicas de distintxs usuarixs. Esto es por que si bien todas las distros de Linux se basan en el mismo núcleo, cada una tiene sus propias características y enfoques.

Hay una gran cantidad de distribuciones, y encontrar una que se adapte a tu uso diario y objetivos es importante (y hasta diviertido :p)! Dejamos una lista de recomendados en orden de facilidad de uso:

• **Linux Mint:** es famosa por su entorno de escritorio clásico y familiar, ideal para quienes quieren sentirse “en casa” tras dejar Windows. Basada en Ubuntu, hereda su estabilidad y compatibilidad. Su interfaz es muy amigabley tiene un excelente rendimiento, ideal para equipos modestos.
https://linuxmint.com/



• **Ubuntu:** es muy facil de usar, posee una comunidad gigantesca y da soporte a largo plazo de muchas de sus versiones. Es muy estable y compatible con casi cualquier equipo, pero puede sentirse algo pesado en equipos antiguos (aun asi, sigue siendo mas liviano que un windows en los mismos equipos)
https://ubuntu.com/

• **Zorin OS:** combina la elegancia visual con la facilidad de uso. Está pensada para quienes buscan una transición suave desde Windows o macOS, con un diseño cuidado y buen rendimiento.
https://zorin.com/os/

• **Antix:** sistema operativo pensado específicamente para computadoras viejas que necesiten una revivida, con lista de aplicaciones open source para instalar directamente (y recursero socialista incluido)
https://antixlinux.com/

• **Cirujantix:** es un Antix especifico para conectar igualdad creado por Cybercirujas. Tiene optimizaciones para computadoras de bajo rendimiento, con disco rígido mecánico

y desde 1GB de memoria RAM, y con intel ATOM N45x, pero es compatible con otros equipos más potentes.
https://cybercirujas.rebelion.digital/foro/viewtopic.php?p=823#p823

• **Loc-OS:** Alternativa a Antix, tambien pensado especificamente para revivir computadoras viejas.
https://loc-os.com/

• **Tails:** Es un sistema operativo portátil, se puede utilizar desde un pendrive conectado a una computadora sin instalar nada. Utiliza la red TOR para protegerte de la vigilancia y la censura.
https://tails.net/install/index.es.html

• **Whonix:** Funciona como una aplicación que maneja toda la actividad en una máquina virtual y fuerza todo el tráfico de Internet a través de la red TOR. Ofrece protección de la privacidad y el anonimato en línea y está disponible para los principales sistemas operativos. Whonix consta de dos partes: una que ejecuta únicamente Tor y actúa como puerta de enlace, que se llama Whonix-Gateway. El otro, que se llama Whonix-Workstation, está en una red completamente aislada. Solo las conexiones a través de Tor son posibles. Con Whonix, puede usar aplicaciones y ejecutar servidores de forma anónima a través de Internet. Las fugas de DNS son imposibles, e incluso el malware con privilegios de root no puede averiguar la IP real del usuario.
https://www.whonix.org/wiki/Download

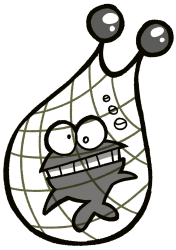
• **Qubes:** Qubes OS es un sistema operativo gratuito y de código abierto, orientado a la seguridad, para la informática de escritorio de un solo usuario. Aprovecha la virtualización basada en Xen para permitir la creación y gestión de compartimentos aislados llamados qubes. Estos qubes se implementan como máquinas virtuales a través de Whonix. Es una solución algo más técnica que las anteriores, y exige computadoras más modernas para ejecutarse.
https://www.qubes-os.org/downloads/

Para encontrar aun más opciones disponibles, podes pispiar por https://distrowatch.com/

Redes Sociales

Recordemos que cuando usamos redes tales como Instagram, Facebook, TikTok, etc., estamos en plataformas que pertenecen a empresas privadas con sus propios intereses. Estas empresas:

• **Centralizan el control y distribución de la información.** Por ejemplo, regulan la noticias que recibimos o dejamos de recibir sobre palestina. Incluso regulan lo que nuestros contactos podrian decirnos o lo que nosotros podemos contarle a nuestros contactos. Frecuentemente, el **shadowbanning** no es solo censura política, sino **optimización de engagement**. El algoritmo "castiga" el contenido que genera desinterés o que no mantiene al usuario en la plataforma (aunque sea contenido legítimo). Esto crea una **censura silenciosa por ineficiencia comercial**, no solo ideológica.



El modelo centralizado con el que trabajan las redes sociales principales es susceptible a un único punto de fallo. Si algo dejara de funcionar en Twitter, este error afectaría a más de 500 millones de cuentas, si falla Instagram, a más de 2 mil millones de cuentas. Esto ya ha sucedido. Por ejemplo, en octubre de 2021, Facebook, Instagram y WhatsApp dejaron de funcionar de manera simultánea por 5 horas a nivel de mundial. Eso quiere decir que miles de millones de personas a nivel global perdieron parte importante de su comunicación por culpa de una sola empresa.

Al depender de infraestructura privada extranjera (servidores en EE.UU. o Europa), los países y comunidades pierden soberanía sobre su propia información. Si una empresa decide cerrar un servicio o bloquear un país, no hay alternativa técnica inmediata.

• **Deterioran la privacidad y seguridad.** Recopilan masivamente, explotan, venden, trafican y cruzan nuestros datos personales, que luego comparten con otras empresas, los gobiernos o la policía.¡Nada es privado! Una buena regla es recordar que todo puede terminar en las manos de la borracha.

• **Capturan nuestra atención, que es la moneda corriente de las plataformas.** Para lograr esto, priorizan modos de uso que generen que pasemos más tiempo en sus plataformas. Esto puede significar, por ejemplo, que veas más publicaciones que te hagan enojar porque eso genera que te quedes más tiempo peleando o que veas muchos posteos desesperanzadores, sólo para que sigas buscando algo que te suba el animo dentro de los mismos reels que te hicieron sentir eso.

• **Pueden causar daño emocional y social**, y de hecho están diseñadas para eso; comparación constante, baja autoestima, cyberbullying, desinformación, aislamiento.

• **Permiten y hasta fomentan la proliferación de desinformación,** noticias falsas y teorías conspirativas. Llevándote siempre al extremo de tu punto de vista; te suelen dar la suficiente recompensa como para que sientas que estas ganando información nueva cuando en realidad solo estas hundiéndote en un pozo de sobre-información y sesgo de confirmación.

Es moneda corriente el uso masivo de **bots** para crear la ilusión de consenso artificial. Si 10,000 cuentas zombi tuitean lo mismo, el algoritmo lo trata como "tendencia", aunque sea falso, ya que lo único que le importa es que sea redituable, no real. Esto distorsiona la realidad pública.

• **Modulan nuestros estados de ánimo y nuestras opiniones.** Incluso, se esta investigando la influencia en, por ejemplo, las elecciones estadounidenses 2020.

Todo esto lo generan para su beneficio comercial y político y el de sus socios. Nosotras, al habitar estos espacios, terminamos siendo en doble instancia **trabajadoras no pagas** de las plataformas. No solo nos agotan nuestra atención, sino que generamos contenido (posts, reels) y datos (interacciones por mensaje, comentarios, likes, incluso el tiempo que nos

detenemos en cada publicación) que la empresa procesa y vende, sin que recibamos compensación económica por ello. Como referencias sobre el tema, Proton genera un informe frecuente sobre ¿Cuanto valen tus datos?

También recomendamos la lectura La era del capitalismo de la vigilancia.

La infraestructura y sistema de moderación de estas redes se sostiene también en el trabajo precarizado de moderadores de contenido en países del Sur Global (como Filipinas o India), quienes sufren trauma psicológico por ver contenido violento o de abuso infantil.

Si queremos seguir usando las redes sociales privativas :(

Recordemos revisar las configuraciones de privacidad de cada plataforma. Hay permisos que las plataformas mantienen difíciles de cambiar o encontrar. Por ejemplo, podemos optar porque la publicidad no esté personalizada.

Ser conscientes de lo que publicamos y compartimos. Nuestras fotos y publicaciones pueden tener metadatos asociados basados en nuestra locación, pero además, las fotos que publicamos pueden tener información sobre los lugares identificables que habitamos y nuestras rutinas o hábitos en ellas.

Incluso podemos pensar en tener mail/número que no sea fácilmente asociado a unx o que sea temporal, como se encuentra explicado en la sección de Correos.

Hay extensiones para nuestros navegadores que bloquean ciertas partes de las plataformas que nos puedan resultar mas problemáticas, como por ejemplo, bloqueadores de shorts en youtube, filtro blanco y negro para instagram, filtro de tweets realizados por personas transfobicas en twitter, bloqueadores de anuncios en videos, etc.

Si bien proponemos dejar de usar las redes capitalistas, también entendemos que en este momento son la plataforma con más llegada a la opinión pública, donde se convierten en un terreno de disputa. Se puede adoptar una estrategia mixta: pero a la vez ir publicando en paralelo en las redes libres y comunitarias, de forma que las personas que estén migrando hacia ellas puedan seguir informándose y difundiendo sin el efecto “entré para ver qué onda y no encontré a nadie”.

Si no tenemos cuenta de alguna red privativa pero queremos ver un enlace que nos mandan, podemos usar Frontends Alternativos. Son apps que reemplazan a la oficial de dicha red y que evitan que enviemos datos.

Para twitter, existe **Nitter.** Twitter ha estado cerrando instancias de Nitter constantemente. Si una no funciona, busca en comunidades de privacidad cuál está activa ese día. Tambien existe https://xcancel.com/

para youtube existe Invidious y NewPipe para celulares. Además, estas apps no tienen anuncios :D

Si queremos alternativas

Recomendamos investigar el fediverso :)

El fediverso es un conjunto de redes sociales que se comunican entre sí gracias a que todas usan un protocolo llamado ActivityPub, es decir, un lenguaje común que permite que desde cualquier punto del fediverso puedas seguir e interactuar con personas en otros puntos del fediverso. Mas o menos como funciona el email: si tenemos una cuenta en Gmail, podemos escribirte a una amiga que tenga su cuenta en Protonmail, y ambas podemos hablarle qa mi tío que solamente usa Riseup.

En el fediverso participan redes federadas como **Mastodon** (que es similar a Twitter), **Pixelfed** (similar a Instagram),

Peertube (a Youtube), entre muchas otras, y al ser redes sociales federadas, te podés unir desde la que quieras y aun asi comunicarte con todas las demás.

Mastodon es solo una de las redes sociales del fediverso, y hay miles servidores de Mastodon. A los servidores les decimos instancias, esto va a tener más sentido cuando te hagas tu cuenta. Cualquiera (con un poco de ganas, tiempo y media compu) puede ponerse su propia instancia, o examinar el código de Mastodon y cambiarle lo que quiera, porque es todo software libre.

Cada servidor se rige según las normas que sus administradoras elijan. Los hay que funcionan de manera asamblearia y entre todas las usuarias deciden cómo se configura, qué contenidos se moderan, etc. Si, por lo que sea, alguien se pone un servidor para hacer cosas maliciosas (como, por ejemplo, hacer spam, publicidad o noticias falsas), la solución es simple: hacés o pedís que tu instancia no se comunique con la maliciosa.

Para mas ayuda con el fediverso, recomendamos visitar el sitio de **https://vamonosjuntas.org/**

También recomendamos explorar el mundo del indieweb <3

La **indieweb** (o como nos gusta decirle, la web tikita jiji) es el movimiento que busca devolver a las personas el control total sobre su identidad digital. Consiste en un espacio donde te podes armar tu propio blogcito, tu propio rincón de la internet. Es completamente personalizable, permitiendo que nos expresemos mucho más que con un perfil preformateado de una Red Social.

Salud y consecuencias

Recordemos que las formas en las que nos manejamos y ien las que convivimos dentro de la virtualidad, afectan también en cómo pensamos y nos manejamos fuera de la imisma.

El impacto en la mente: Estrés, Adicción y Sobrecarga

Es importante tener en cuenta que emociones nos genera, por ejemplo, leer twitter. Tenemos que preguntarnos: ¿A quién le conviene que estemos enojades? Como explicamos en el apartado de redes sociales, el diseño de las plataformas prioriza el contenido que genera reacciones fuertes (enojo, indignación, miedo) porque retiene la atención.

Esto activa nuestro sistema nervioso simpático, elevando el cortisol y la adrenalina. Pasar horas en este estado nos mantiene en un ciclo de estrés crónico. Esto no solo nos agota, sino que debilita nuestro sistema inmunológico, altera el sueño y reduce nuestra capacidad de empatía y calma.

Antes, la información la buscábamos nosotres (intención activa). Ahora, el algoritmo la entrega (intención pasiva). Esto genera fatiga de decisión y sobrecarga informativa. Nuestro cerebro gasta energía filtrando lo que nos interesa y lo que no.

Al estar constantemente filtrando el ruido, se reduce nuestra capacidad de concentración profunda y aumenta la sensación de **"niebla mental"**: dificultad para pensar co olvidar cosas simples y sentirse saturadx aunque no hayas hecho algo.

Además, al no buscar activamente, el algoritmo nos muestra solo lo que confirma nuestras creencias o lo que nos enoja. Esto polariza la sociedad y nos des-regula el termométro de la realidad. Dejar de buscar y tener curiosidad es una forma de dejar de pensar críticamente. Si no sé de dónde viene la información o por qué la estoy viendo, no puedo evaluar su veracidad ni su contexto.

Además, las apps usan el mismo principio que las máquinas tragamonedas: no sabes cuándo llegarán los "likes" o las notificaciones, cuando el reel va a ser aburrido o cuando lo mejor que te pasó. Esta incertidumbre crea una adicción conductual similar a la de las apuestas, donde la dopamina no viene del contenido, sino de la anticipación de la recompensa, que no llega de manera fiable. Este es el diseño de Intermitent Variable Rewards (refuerzos variables intermitentes).

Apuestas

Si las redes sociales y el celu ya nos producen adicción, ni hablar de las plataformas que son literalmente de apuestas. Según datos de UNICEF Argentina:

- 1 de cada 4 chicxs argentinxs de entre 12 y 17 años ha apostado online al menos una vez.
- El 16% de los estudiantes de secundaria visita frecuentemente páginas de apuestas.

Estas plataformas no solo muestran apuestas deportivas; están conectadas a casinos online propios. Puedes saltar de apostar por Francia versus Paraguay a jugar a la ruleta en dos clics. El Mundial 2026 fue una gran oportunidad: Betano es el promotor oficial de la AFA, ofreciendo "recompensas" y promociones ligadas a los resultados. La línea 141 del CENAD (Centro Nacional de Atención de las Adicciones) recibió un 27% más de llamadas por juego compulsivo el año pasado.

¿Qué se puede hacer?

Para romper con los ciclo de inercia, recomendamos preguntarnos antes de entrar:

- ¿Qué necesito de esto?
- ¿Estoy aburridx, ansiosx, enojadx o buscando conexión?
- ¿Tengo tiempo real para esto o estoy escapando de una tarea pendiente?

Identificar la emoción que nos lleva a abrir la app nos devuelve el control y nos permite decidir conscientemente si entramos o no, en lugar de caer en el hábito automático. Es importante recordar igual el contexto en el cual tenemos estos sentimientos, y que si seguimos “cayendo” en estas conductas es porque la plataforma está hecha literariamente para que “caigamos”.

No es un problema de falta de voluntad, estamos peleando contra una maquinaria diseñada por miles de ingenierxs, psicólogxs y data scientist que literalmente intentan quitarnos nuestras horas de descanso.

Recomendamos como lectura estos dos textos amigos sobre adiccion al celular y una caja de herramientas para mitigarlo.

https://texto-plano.xyz/revista/002/07_adiccion.html

https://texto-plano.xyz/revista/004/06_3_adiccion_celular.html

La cuerpa

Estar sentade o tirade en la cama mucho tiempo nos hace mal a la cuerpa. Las consecuencias en salud no son solo mentales, si no que también tiene influencia en nuestra postura, espalda, ojos y sueño.

> Mirar una pantalla cercana por horas es un esfuerzo

enorme para nuestros ojos. El parpadeo disminuye drásticamente al mirar pantallas (pasamos de parpadear 15-20 veces por minuto a solo 5-7), lo que causa sequedad, irritación y esa sensación de "arena" en los ojos. La recomendacion de oftalmologues a la hora de mirar pantallas por un tiempo prolongado es pausar cada 10 minutos y mirar a la distancia para descansar la vista. Tambien existen lentes con filtro azul o de descanso puede ayudar a reducir la fatiga, pero lo más importante es la pausa y la distancia.

> Al estar sentades en la cama o en sillas malas, la espalda se nos curva hacia adelante. Esto comprime nuestros discos intervertebrales y tensa los músculos del cuello y los hombros. Existen ejercicios en youtube especificos para las que trabajamos esas horribles 9 horas sentadxs.

> La luz azul emitida por las pantallas inhibe la producción de melatonina (la hormona que regula el sueño). Además de la luz, el contenido emocional (noticias graves, discusiones, dramas) mantiene el cerebro en estado de alerta (cortisol alto), lo que impide la relajación necesaria para conciliar el sueño. Recomendamos activar el filtro de luz azul en tus dispositivos desde 1 hora antes de dormir y dejar el celular cargando en otra habitación.

Autonomía Cognitiva y Contexto de Lucha

Los conflictos actuales, si bien menos signados por la promesa de aniquilación mutua o un invierno nuclear no dejan por ello de ser preocupantes, mientras vemos como la posibilidad de una tercera guerra mundial se extingue como el sol en el horizonte, se alzan lunas y estrellas proclamando la llegada de una segunda guerra fría.

Un conflicto caracterizado por la capacidad de construir

esferas de influencia, capturar aparatos estatales e incorporarlos a un armado imperial mientras se genera negación plausible de los actos y se esquivan tanto regulaciones como sanciones internacionales.

Ante esto vemos emerger actores constituidos como extensiones de las potencias imperiales que responden a la necesidad de expandir las capacidades de las potencias imperiales, en la forma de participación entre estados pero sobretodo como empresas que prestan servicios a los estados.

Puesto que en un conflicto de estas características la frontera entre los asuntos internos y externos se vuelve particularmente difusa nos referiremos a las actividades como centradas en uno de dos frentes pero estos están tan integrados que también podría leerse como distintas etapas de un proceso.

En el caso de expandir las capacidades imperiales externas se puede pensar en empresas de seguridad que operan asegurando complejos de extracción o refinamiento en países en conflicto, mas conocidos como mercenarios o empresas de inteligencia privada como nso group o pinkerton group que habilitan técnica y operativamente el espionaje en estados que carecen de esas capacidades o que deciden no ejercerlas directamente.

En el caso de expandir la capacidades imperiales internas, se puede pensar en empresas cuya función es recolectar de forma masiva y sistemática datos, generar modelos para predecir e influir en el comportamiento. destinados a ser implementados por un lado como técnicas de represión y por el otro como técnicas de desestabilización, siendo nuestra concepción del mundo tanto materia prima como campo de batalla, privándonos de nuestra agencia.

Frente a semejante ataque proponemos un curso accionable que empieza por dejar de alimentar estos sistemas mediante la entrega voluntaria de nuestros datos, la construcción de

alternativas comunitarias, libres y respetuosas,la difusión de técnicas y conocimientos autonomizadores pero sobretodo la abolición de la publicidad como industria y la propiedad intelectual como figura legal.

El Colonialismo Digital: El idioma, la cultura, la infraestructura

El contenido generado en la internet y lo que consumimos está mayoritariamente pensado en otro idioma, para otro país.

Yankilandia tiene formas de pensar y maniobrar muy individualistas y basadas en sus creencias. Tiene una matriz cultural profundamente individualista, basada en la meritocracia extrema, la fe en el mercado y una visión del mundo binaria. Cuando vemos, leemos e intercambiamos con contenido basado en esas filosofias de vida, como las estamos incorporando como una verdad base? Como empezamos a pensar, por ejemplo, la forma de politica que tienen alla como la verdadera forma de hacer o pensar politica? El estandar global se vuelve el estándar estadounidense.

Si buscás recursos sobre electrónica, programación o arte

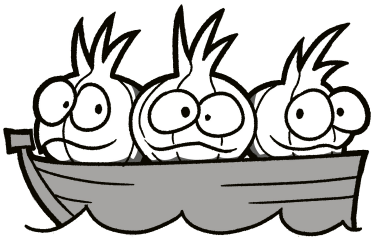
digital, y los manuales, tutoriales y comunidades están mayoritatiamenrte en inglés. Las que sabemos el idioma, nos acostumbramos a buscar cosas en ingles, cambiar el idioma de la wikipedia, siempre esperar estos recursos como "mejor hechos". ¿Por qué?

El internet no es "nube" etérea; son cables de fibra óptica bajo el océano, servidores en data centers y protocolos que se deciden en foros dominados por empresas de EE.UU. y Europa.

Si un gobierno extranjero decide bloquear una red, o si una empresa decide dejar de dar soporte, **nuestra vida digital se detiene**.

No tenemos "backup" nacional. No tenemos nuestra propia versión de Google, de Facebook o de los protocolos de internet. Somos inquilinos en la casa de otros.

Libros que expanden sobre los temas:



Hipótesis cibernética | Tiqqun

A nuestros amigos (2014) | Comité invisible

Saskia Sassen – Expulsión

Byung-Chul Han – La Sociedad del Cansancio

Siva Vaidhyanathan – La Googlizacion de todo

Utopías digitales: Imaginar el fin del capitalismo – Ekaitz Cancela

Guerras de internet: Un viaje al centro de la red para entender cómo afecta tu vida – Natalia Zuazo

Protocol: How Control Exists after Decentralization – Alexander R. Galloway

Tubes: A Journey to the Center of the Internet – Andrew Blum

Cybertypes: Race, Ethnicity, and Identity on the Internet – Lisa Nakamura

Privacidad General

En nuestra interacción con el mundo virtual, estamos constantemente dejando rastros que revelan no solo qué hacemos, sino también nuestras tendencias, gustos y hábitos, nuestra ubicación, nuestras personas cercanas, y mucho más. Para ocultar esos rastros, es clave que entendamos los distintos mecanismos de vigilancia y utilicemos las herramientas correctas para cada uno.

¿Me estan espiando?

Casi todos los sitios web tienen alojada tecnología que nos identifica y rastrea (Cookies de terceros, píxeles invisibles, logins de instagram y tiktok, Google Analytics, etc.). Para descubrir que tecnologías usan los sitios que conocés y entender mas sobre cada una podes usar **Blacklight** (https://themarkup.org/blacklight). Ingresas una direccion web y Blacklight la abre para revelar las tecnologías de seguimiento que contiene. Te muestra exactamente quién está obteniendo tus datos y con qué propósito. Esto te ayuda a tomar decisiones informadas sobre en qué sitios confías y cuáles evitas.

Las VPN

Una VPN (Red Privada Virtual) nos permite crear una conexión segura y cifrada entre nuestro dispositivo y un servidor en cualquier otra parte del mundo. Todos los datos que sin VPN se verían saliendo desde nuestros dispositivos, pasan como por un tubo hacia el servidor de nuestra VPN para luego salir mezclados con los datos de tod@s l@s otras personas que esten usando el mismo punto de salida.

Así le ocultamos nuestra verdadera dirección IP a los sitios que visitamos y evitamos que nuestros proveedores de internet, DNSs y otrxs en nuestra red puedan rastrear nuestras actividades. Por esto ultimo decimos que las VPNs mejoran nuestra seguridad cuando usamos redes públicas.

También podemos usar VPNs para acceder a contenido que está bloqueado geográficamente. Al poder salir a internet como si estuviésemos en otros países, evitamos algunos bloqueos regionales.

Recomendamos:

- **RiseupVPN** para un uso general y moderado, una opción de código abierto y sin registros (no-logs) que prioriza la privacidad.

- **Mullvad VPN** destaca por soporte WireGuard, port forwarding remoto y pagos anónimos.

- **NordVPN** es una opción (paga) muy recomendada ya que (hasta el dia de hoy) parece solo una vez haber entregado a autoridades gubernamentales información sobre sus usuaries.

Es muy importante tener en cuenta que estaríamos depositando en nuestro proveedor VPN toda la confianza que no le tenemos a nuestros proveedores de internet, nuestros DNS o la red en la que nos encontramos.

¿Por qué sería mejor confiar en una VPN?

Porque los proveedores de Internet por lo general están

obligados por ley a guardar registros de sus usuarios. Podemos elegir un proveedor de VPN en un país que no tengan ley de retención de datos personales. Antes de elegir por un proveedor, recomendamos buscar noticias de si alguna vez entregaron datos ante una orden judicial.

El DNS

El DNS (Sistema de Nombres de Dominio) es el "directorio" de internet que traduce nombres de sitios (ej. `google.com`) a direcciones IP para que podamos ir a visitar sitios usando su nombre en lugar de una serie de números y puntos.

Por lo general, las consultas y respuestas a un DNS se envían en texto plano (a través del protocolo UDP), lo que significa que pueden ser leídas por nuestro ISP (fibertel, claro, iPlan), personas en nuestra misma red, o cualquiera que pueda supervisar nuestras transmisiones. Incluso cuando un sitio web utiliza HTTPS, la consulta de DNS para llegar a ese sitio web queda expuesta. Eso significa que aun si no saben que es lo que “hablamos” con un sitio web, se puede saber con quien hablamos, cuanto, cuantas veces y por cuanto tiempo.

DNS sobre TLS (DoT) y DNS sobre HTTPS (DoH) son dos estándares diseñados para cifrar el tráfico de DNS, ocultando qué sitios consultas a tu proveedor de internet (ISP).

En **Firefox** las opciones estan disponibles para usar DoH con Cloudflare o NextDNS, pero no estan activadas por defecto. Al igual que otros navegadores, requieren activarse manualmente.

Desde el punto de vista de la privacidad, DoH suele ser la opción preferible. Al encapsular las consultas dentro del tráfico estándar de HTTPS, se mezclan con el resto de la navegación web, lo que dificulta su detección o bloqueo por parte de terceros.

Sin embargo, es crucial evitar las **filtraciones DNS** al usar una VPN. Esto ocurre cuando el sistema operativo o el navegador ignoran la configuración de la VPN y envían las consultas DNS directamente al servidor del ISP, fuera del túnel cifrado. Como resultado, aunque tu tráfico web esté protegido, el ISP (o cualquiera que monitoree la red) puede ver exactamente qué dominios estás visitando.

Para comprobar que no existen filtraciones DNS en nuestras VPNs recomendamos testear **dnsleaktest** (https://www.dnsleaktest.com/) mientras tenemos la VPN activa. Si el test muestra servidores DNS de tu país o de tu ISP (y no los de la VPN), tienes una filtración DNS. En ese caso, configura manualmente el DNS dentro de tu aplicación de VPN o cambia de proveedor.

Limpiar metadatos

Primero: ¿Que %@#$ es un metadato?

Los metadatos son datos que describen otros datos, proporcionando información sobre su origen, contenido, contexto o forma de manejo.

Mas despacio por favor...

Si el dato es una **foto** que sacaste con tu celu: sus metadatos pueden ser la cámara que se usó (que revela que celu tenes), la velocidad de obturación y la apertura del foco, y también la ubicación según el GPS de tu celu cuando sacaste la foto.

Si el dato es un **documento** de tu word en tu windows: sus metadatos pueden ser el usuario que lo guardó, su versión de word, cuando editó el documento por última vez, etc.

Y, si el dato es un **mensaje** por whatsapp: sus metadatos pueden ser quien lo envió a quien, si es original o reenviado, si contiene adjuntos, a que hora se envió, etc.

Aunque muchas plataformas te digan que el mensaje que

mandaste está encriptado, si guardan el cuando, como, a quien, que tan frecuente, desde donde lo mandaste, etc, están guardando información que quizás no quieras compartir.

Si alguien posee un montón de datos similares de sistemas de mensajería similares donde ni los datos ni los metadatos están desencriptados, creemos que podría revelar con bastante certeza el contenido de tus conversaciones a partir de tus metadatos. (comentario inocuo al pasar, desde el 8 de mayo de 2026, Instagram, que pertenece a Meta, que también es dueña de Whatsapp desactivó el cifrado de extremo a extremo en los mensajes directos “Para entrenar sus modelos de IA”) (ver otras opciones en la sección de mensajería).

Ahora sí, a lo que vinimos

Una herramienta recomendable para limpiar metadatos es ExifTool. Está disponible para Windows, macOS y Linux. Aunque se puede usar sin instalar (descargando el ejecutable), recomendamos instalarla para tener uso completo de sus funciones desde la línea de comandos.

Existen guias de uso en internet y también tenemos varios ejemplos en la versión de este recursero en:
www.partidopirata.com.ar/recursero-gt/

Seguridad general

Antes de hablar de las mitigaciones con herramientas y tecnología, es importante tener en cuenta que un factor muy inseguro somos... nosotrxs. No importa las prácticas de seguridad que te sepas, sólo hace falta estar medio dormida un día para hacer clic en la pagina que no era, o hacer un chiste incorrecto en un grupo muy público de la toma de la facu. También está bueno hacerle cada tanto una limpieza al

celu de cosas muy queme, es una muy bella practica!

Conoce las tecnologías de vigilancia que nuestrxs amigxs, las fuerzas del orden, utilizan para conocernos mejor.. ¡son tan amorosxs! Guía de campo sobre la vigilancia policial Aunque está basado en nuestra madre patria del norte, mucho de este material es perfectamente aplicable a nuestra realidad.

Muchas veces la complejidad de abordar una estrategia de seguridad nos juega en contra y puede terminar haciéndonos optar por no abordar el problema en absoluto. Por suerte, toda complejidad puede separarse en problemas más pequeños y accesibles.

Un gran trabajo en simplificar estos conceptos y volverlos más manejables lo hizo la EFF, una fundación sin fines de lucro con el objetivo de proteger la privacidad en línea. Podemos acceder a sus artículos contra la vigilancia masiva en: https://ssd.eff.org/es/

Limpiar documentos adjuntos

Abrir un archivo adjunto de alguien que no conocemos o que no sabemos si nos envió a propósito es una de las formas más comunes de infectarnos un dispositivo.

Los adjuntos pueden contener código malicioso, macros ocultas o rastreadores que se activan al abrirlos. Para neutralizarlos podemos usar herramientas que "sanean" el contenido manteniendo la legibilidad.

Dangerzone (https://dangerzone.rocks/) es una herramienta de código abierto diseñada específicamente para este fin.

Su proceso es robusto y seguro:

• **Sandboxing (Aislamiento):** El documento entra en un entorno aislado (sandbox) donde no puede dañar tu sistema principal.

• **Descomposición:** Dangerzone convierte el documento (ya sea PDF, Office, imagen, etc.) en una imagen pura (píxeles RGB). En este paso, todo el código ejecutable, las macros y los scripts ocultos se destruyen porque dejan de ser "código" y pasan a ser solo "colores".

• **Reconstrucción:** En un segundo sandbox, esos píxeles se convierten nuevamente en un PDF limpio.

• **Resultado:** Obtenés un PDF visualmente idéntico al original, pero 100% inerte. No puede ejecutar nada, no tiene enlaces activos (podés reactivarlos si querés) y no contiene rastreadores.

• **Compatibilidad:** Disponible para Linux, Windows y macOS.

• **Limitación:** Funciona excelentemente con PDFs, documentos de texto (Word/LibreOffice) e imágenes. No funciona bien con planillas de cálculo (Excel/Calc) porque la estructura de datos tabulares se pierde al convertirla en imagen.

Otra alternativa es utilizar una Maquina Virtual (VM), que emula un espacio apartado y aislado de tu computadora y datos. Podes leer mas aquí: https://www.welivesecurity.com/la-es/2017/03/30/entorno-virtual-pruebas-con-malware/

BackUps

Nuestros datos son una de las cosas mas valiosas que tenemos. Consideramos que es importante no dejar nuestra memoria digital en manos de corporaciones o en un ecosistema donde las plataformas privadas pueden borrar nuestras cuentas, censurar contenido o sufrir brechas de seguridad.

Algunas practicas de backup son:

La Regla 3-2-1:

3 copias de tus datos (original + 2 backups).

2 medios de almacenamiento distintos (ej. disco duro local + nube o disco externo).

1 copia fuera de tu ubicación física (nube o disco en otra casa) para protegerte de robos, incendios o inundaciones.

• **Cifrado Local: Recomendamos que no subas datos desencriptados a la nube.** Aunque el proveedor diga que "no lee tus archivos", la infraestructura está en manos de terceros con intereses comerciales o políticos. Se pueden usar herramientas de cifrado de disco como **LUKS (Linux)**, **FileVault (macOS)** o, para archivos individuales, **GPG o Cryptomator (que crea un "vault" cifrado en la nube)**.

• **Realizar pruebas de verificación.** No hay nada peor que probar la validez de un backup cuando hay una urgencia y descubrir que no funciona. Para evitarlo, periódicamente revisemos la salud de los mismos.

Si podemos abandonar las nubes del mal por algo mas casero, recomendamos administrar los backups con el Borg:

BorgBackup (https://www.borgbackup.org/)

Le recomendamos por que es de código abierto, por que que utiliza deduplicación (una técnica que identifica y elimina las copias duplicadas de los datos para que cada cosa que pueda estar repetida se almacene una sola vez.) También usa compresión previo a la encriptación del lado del cliente. Permite almacenar data en cualquier host remoto accesible via SSH y Detecta y repara corrupción de datos de forma automática, asegurando que tu backup sea fiable a largo plazo.

Si vamos a seguir usando alguna nube para resguardar nuestra informacion, recomendamos siempre encriptarla previamente con:

VeraCrypt (https://www.veracrypt.fr/)

VeraCrypt es una herramienta que implementa el concepto de OTFE (On The Fly Encryption - significa que los datos son accesibles de forma inmediata, luego de haber ingresado la correspondiente clave de descifrado). Es software de código abierto, y funciona tanto en Windows, como en GNU/Linux y Mac. Se pueden cifrar archivos, particiones e incluso discos enteros. Es recomendable utilizar las opciones esteganográficas (volumen oculto, sistema operativo oculto).

Contraseñas

Sabemos que da una fiaca tremenda y que es agotador tener que recordarlas, pero es importante tener contraseñas fuertes, no reutilizarlas y estar atentxs a que las mismas no sean vulneradas.

Si una plataforma sufre una filtración de datos y usaste la misma contraseña en tu correo, banco o redes, todas esas cuentas quedan comprometidas de golpe.

¿Qué recomendamos?

Primero, recomendamos que generes contraseñas seguras y utilices un **gestor de contraseñas** (podes leer más en profundiad en: Cómo crear contraseñas seguras).

Recomendamos fuertemente el uso de un gestor de contraseñas, que es una aplicación que genera, guarda y rellena automáticamente tus credenciales de forma segura.

Recomendado: KeePassXC

• Es de código abierto, gratuito y funciona localmente en tu dispositivo (no depende de la nube).

• Creas una base de datos (archivo) protegida por una única contraseña maestra muy fuerte.

• Para el resto, el gestor genera cadenas aleatorias de 20+ caracteres que tú nunca necesitas recordar.

• Ventaja: Si pierdes el acceso a tu correo, no pierdes el acceso a tus cuentas, porque tus claves viven en tu archivo local, no en un servidor de terceros.

Además, activar la **autenticación en dos pasos (2FA)** añade una capa extra de seguridad.

No recomendamos 2FA por SMS. Hay que tener en cuenta que los códigos por SMS son vulnerables a ataques de SIM Swapping (donde un atacante convence a tu operadora de mover tu número a otra tarjeta).

Aplicaciones como **Aegis, Authy** o la integrada en tu gestor de contraseñas generan códigos de 6 dígitos que cambian cada 30 segundos. Estos códigos no pasan por la red telefónica ni por servidores de terceros, lo que los hace mucho más seguros.

¿Cómo se si mi contraseña ya fue expuesta?

Se puede verificar si un mail tiene contraseñas expuestas en el sitio **haveibeenpwned** (https://haveibeenpwned.com/). **"Pwned"** viene de la palabra "owned" (poseído/comprometido). HIBP es un buscador que recopila bases de datos de contraseñas y correos que han sido robados en grandes brechas de seguridad (como la de LinkedIn, Adobe, etc.) a lo largo de los años.

Si aparece nuestra contraseña, corremos un riesgo. Toca cambiar la contraseña del servicio afectado, revisar si la reutilizamos para otro servicio y cambiarla ahí también.

Celulares

Hay que tener en cuenta que suele ser mucho más difícil mitigar y cuidarse en el celular, ya que es mucho más vulnerable que una pc. Hay prácticas importantes a tener en cuenta:

- **Configurar una contraseña para encender.** En Android, se puede configurar desde **Ajustes → Seguridad y privacidad → Bloqueo de pantalla** (el nombre de las opciones puede variar según el modelo).

- **Encriptar dispositivo.** La mayoría de los celulares modernos utilizan cifrado de almacenamiento de forma predeterminada. Para comprobarlo, revisar **Ajustes → Seguridad y privacidad** o buscar "cifrado" en los ajustes del teléfono. Si el dispositivo permite activarlo manualmente, hacerlo y mantener actualizado el sistema operativo.

- **Encriptar memoria SD.** Si el celular utiliza una tarjeta SD, comprobar en **Ajustes → Seguridad** si existe una opción para cifrarla. El cifrado protege los archivos de la tarjeta si esta se extrae y se conecta a otro dispositivo.

En la pantalla de bloqueo puede ser tentador desbloquear con la huella, pero hay varias cosas a considerar.

Por un lado, como punto negativo, la información de la huella digital la puede recibir y almacenar Google o el fabricante del dispositivo.

Por otro lado, como positivo, podemos pensar que es seguro ya que nadie puede robarte tu huella digital. Sin embargo, en casos de detención, es mas fácil forzarte a poner el dedo qué una clave de 8 numeros. Una mitigación posible a esta situación:

- No llevar el celu (o llevar otro) a marchas.

• Desactivar la opción de desbloqueo por huella antes de ir a una marcha.

Apagar el celu si consideramos posible que haya una detención.

Algunas apps interesantes

Se recomienda instalarlas siempre desde F-Droid que es una tienda de aplicaciones abiertas y libres.

• **Aegis** Permite implementar autenticación de 2 factores (2FA)

• **Briar** Facilita la comunicación con contactos cercanos mediante bluetooth o la señal inalámbrica de un router sin necesidad de conexión a Internet. Es P2P, es decir, no necesita de un servidor centralizado

• **Orbot** Funciona como una VPN a través de Tor. Permite seleccionar que apps querés anonimizar y cuales no.

• **Circulo** Permite crear un canal seguro de comunicación cerrado para un grupo de confianza. Se pueden intercambiar alertas, ubicación, imágenes, etc.

• **Obscuracam** Permite pixelar rostros y vestimentas para no revelar identidades al compartir fotografías

• **Scrambled** Exif Permite borrar los metadatos de una imagen para que su origen no sea detectable

• **OsmAnd** Utiliza GPS sobre un mapa que debemos descargar, evitando entregar esa info a Google u otros al consultar nuestra localización. Al descargar los mapas, no necesitamos conexión a Internet. Por default, utiliza openstreetmap

• **Silence** Permite cifrar SMS (mensajes de texto)

• **Lock Screen** Es una app recomendable para bloqueo de pantalla. Si corremos peligro que nos saquen el celular, esta app es un acceso directo para bloquear la pantalla.

• **Extirparter** Es una app de borrado seguro. Evita la recuperación de archivos eliminados.

• **EDS Lite** Permite almacenar archivos en un contenedor cifrado. Soporta los formatos de contenedor de VeraCrypt y LUKS entre otros.

• **Checkey Checkear** la firma y el los scans de virustotal de las apps que tenemos instaladas

Como chequear si nuestros celulares están pinchados

Para usuarixs con algunos conocimientos técnicos

Drozer (https://github.com/ReversecLabs/drozer) es un framework de pruebas de seguridad para Android. Te permite buscar vulnerabilidades de seguridad en aplicaciones y dispositivos.

MVT https://github.com/mvt-project/mvt Mobile Verification Toolkit (MVT) es una colección de utilidades para simplificar y automatizar el proceso de recopilación de rastros forenses útiles para identificar un posible compromiso de los dispositivos Android e iOS. Desarrollado por Amnesty International como respuesta al **Proyecto Pegasus**.

Phishing y los paquetes mágicos de mercadolibre que nunca pediste

Existe un mito peligroso en la seguridad digital: que el phishing solo le pasa a "gente que no sabe de tecnología" o a usuarios mayores. La realidad es muy distinta. No importa cuántos cursos de ciberseguridad hayas tomado ni cuántas capas de protección tengas; **el eslabón más débil siempre es el humano.**

El phishing no explota fallos de software, explota fallos de estado anímico. Aprovecha el momento en que estás apuradx, cansadx (luego de una jornada agotadora) o sorprendidx (un mensaje de alguien que crees que es de confianza). En esos

segundos de baja guardia, un clic puede costarte caro.

¿Sabes detectar un ataque?

Antes de unos consejos, te invitamos a poner a prueba tu instinto. Podés encontrar algunos **Test de Phishing** online.

¿Cómo te encuentran?

Las vías de entrada más comunes son:

- **Emails de phishing:** El clásico "su paquete está retenido" o "su cuenta será suspendida".
- **SMS (Smishing):** Mensajes de texto que imitan a bancos, courier o servicios de streaming.
- **Mensajes de confianza:** Hackean la cuenta de un amigo o familiar y te piden algo urgente desde ese canal.
- **Anuncios maliciosos:** Publicidad en redes o webs que, al hacer clic, te redirigen a sitios falsos o instalan malware.
- **Notificaciones emergentes:** Pop-ups que simulan ser alertas de tu navegador o sistema operativo ("¡Tu PC tiene un virus! Haz clic aquí para limpiarlo").

Prevención: Herramientas y Prácticas

La prevención es una práctica de verificación activa.

1. Analizá antes de hacer clic

Revisá la URL: No mires el texto visible, mira la barra de direcciones. ¿La ortografía es perfecta? ¿Son dominios raros (ej. `mercadolivre.com` en vez de `mercadolibre.com`)?

Verificá el dominio: Si una URL te parece sospechosa pero no estás segurx, cópiala y pégala en servicios de análisis:

- **VirusTotal:** Te dice si el enlace o archivo es conocido como malicioso.

• **URLVoid:** Te muestra el Whois (quién registró el dominio) y cuándo fue creado. Si un dominio de "MercadoLibre" fue registrado hace 3 días, es una estafa.

Si me mandan un mensaje para entrar a la web de mi banco, vale la pena tomarse unos minutos para entrar "manualmente" (desde los favoritos, buscando el link oficial en tu buscador de confianza) en vez de clickear el link rápido.

2. El "Paquete Mágico" de MercadoLibre/Temu/Correo Argentino

Es una de las estafas más comunes en la región. Te llega un email o mensaje de WhatsApp diciendo que tu paquete fue retenido por aduana o que falta un pago de $500.

La señal de alerta: Ninguna de estas plataformas te pide pagos por WhatsApp, ni te da enlaces para "liberar" paquetes en PDFs o páginas externas.

La acción: Cerrá el mensaje. Entrá manualmente a la app o web oficial y revisá el estado de tus pedidos. Si no aparece nada ahí, el mensaje es falso.

3. Verificá los canales de confianza

Si una amistad te pide dinero o un link urgente, no hagas click ya mismo. Llamá o escribile por otro medio para confirmar que es elle y que no le hackearon la cuenta.

4. Desconfía de la urgencia

El phishing siempre crea un sentido de urgencia: "Tenés 24 horas", "Tu cuenta será cerrada hoy". Los servicios legítimos (bancos, correos, plataformas) rara vez te presionan con plazos tan cortos a través de canales no oficiales. Tómate tu tiempo. La calma es tu mejor firewall.

En el recursero completo de https://partidopirata.com.ar/recursero-gt/ hay más recomendaciones para evitar los ataques de phishing :)

Doxeo

El doxeo (o doxxing) es la práctica de investigar y publicar información personal, privada o confidencial de una persona sin su consentimiento, generalmente con la intención de causar daño, intimidación o acoso.

Los tipos más comunes de doxeo son:

• Publicación online de información personal y privada de una persona con el fin de dañar la reputación de la víctima, así como la de sus familiares, amigxs y/o conocidxs.

• Incitación al acoso y la intimidación de la víctima. Creación de hilos o campañas organizadas para que terceros acosen, amenacen o intimiden a la víctima.

• Doxeo periodístico, uso de esta técnica por parte de medios o periodistas para revelar la identidad de fuentes anónimas o activistas, a menudo bajo la justificación del "interés público", pero que erosiona la posibilidad de hablar libremente en la red.

Recomendaciones y Prácticas de Prevención

La prevención del doxeo se basa en la minimización de la huella digital y la separación de identidades.

• Evita publicar detalles geolocalizados precisos (como la fachada de tu casa, tu placa de auto o el nombre de tu escuela) en redes sociales.

• Borra metadatos de fotos antes de subirlas (Ver sección de metadatos).

• No uses tu identidad principal (tu nombre real, tu email personal, tu foto de perfil) para participar en temas sensibles, activismo o comunidades donde el riesgo de doxeo es alto.

• Creá identidades secundarias ("burners") con emails temporales o alias, sin vincularlas a tu identidad real mediante datos biográficos comunes.

• Revisá la configuración de privacidad de todas tus redes.

Asegúrate de que tu perfil no sea público y que no se pueda buscar por tu correo o número de teléfono.

- Desactivá la opción que permite a otras personas ver quién te sigue o con quién interactúas.

- Si encontrás información errónea o que no deseas que sea pública, utilizá los derechos de supresión que ofrecen algunos sitios o plataformas.

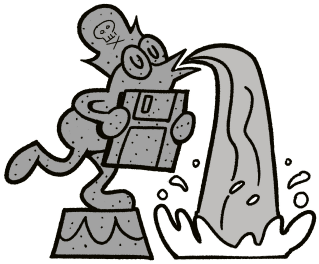
Protegerse del doxeo requiere una combinación de higiene digital, uso de herramientas de privacidad y una conciencia crítica sobre cómo nuestros datos son explotados por el sistema. No podemos controlar todo lo que los demás hacen con nuestros datos, pero podemos minimizar la superficie de ataque y proteger nuestra identidad cuando lo necesitemos.

Sin embargo, es importante recordar que el doxeo suele suceder en un contexto de asimetría de poder y en un contexto donde las redes sociales facilitan el doxeo al permitir la búsqueda pública de perfiles, la geolocalización de publicaciones y la acumulación de datos sin fines claros.

Su modelo de negocio se basa en la vigilancia, lo que las hace cómplices y facilitadoras de esta violencia. Combatir el doxeo no es solo una cuestión técnica, sino política.

mplica exigir regulaciones de privacidad más estrictas, apoyar plataformas descentralizadas que no acumulen datos, y promover una cultura digital que respete la privacidad y la dignidad de las personas.

Fuentes
Fuentes
Fuentes
Fuentes
Fuentes



Lily Jamali (2024) “Telegram ahora proveerá alguna informacion de usuario a autoridades” BBC News https://www.bbc.com/news/articles/cvglp0xny3eo

Jack Schofield (2008) “Problemas de privacidad de Google Chrome, y tips de usuarie” The Guardian https://www.theguardian.com/technology/blog/2008/sep/04/googlechromeprivacyissuesa

Thuy Duong (2026) “Las redes sociales mas populares globalmente en Octubre de 2025, segun cantidad de usuarios mensuales activos” Statista https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Hunt Allcott, Matthew Gentzkow (2024) “Los efecros de Facebook e Instagram sobre las elecciones de 2020: Un experimento de desactivación” https://www.pnas.org/doi/10.1073/pnas.2321584121

https://proton.me/blog/what-is-your-data-worth

https://perio.unlp.edu.ar/catedras/tpm/wp-content/uploads/sites/210/2023/06/ZUBOFF_1.pdf

https://medium.com/new-writers-welcome/the-hidden-costs-of-social-media-that-we-do-not-realize-ecef453a7499

https://www.bbc.com/news/articles/crr9q2jz7y0o

https://pmc.ncbi.nlm.nih.gov/articles/PMC12108933/

https://www.unicef.org/argentina/apuestas-online-salud-mental

https://www.argentina.gob.ar/noticias/la-linea-141-de-la-sedronar-recibio-mas-de-23-mil-llamados-en-lo-que-va-del-2026

https://www.fastcompany.com/4049193 9/netflix-ceo-reed-hastings-sleep-is-our-competition

https://texto-plano.xyz/revista/002/07_adiccion.html

https://texto-plano.xyz/revista 004/06_3_adiccion_celular.html

https://www.infobae.com/tecno/2026/05/08/desde-hoy-tus-mensajes-en-instagram-ya-no-estan-cifrados-asi-afecta-tu-privacidad/

https://sls.eff.org/es/

https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras

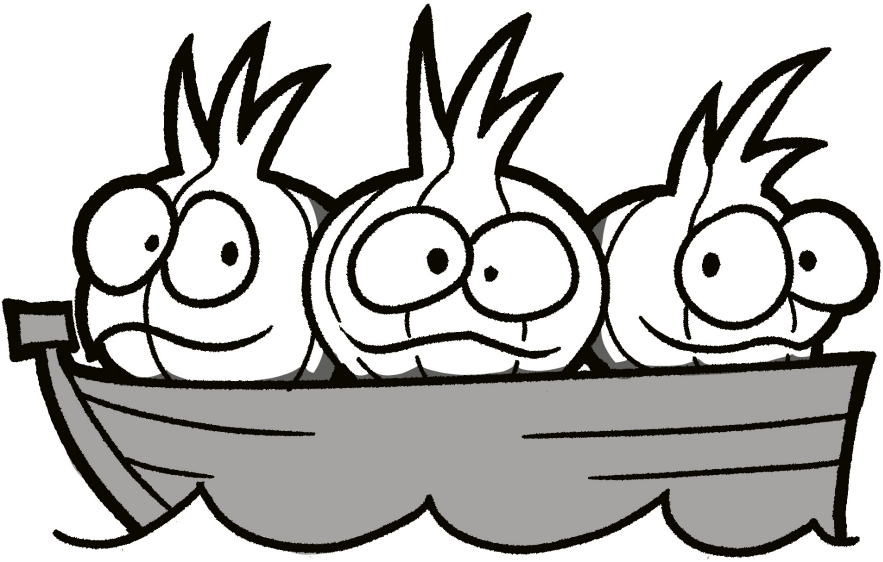
https://forbiddenstories.org/about-the-pegasus-project/
sd.eff.org/es/module/creando-contrase%C3%B1as-seguras

https://forbiddenstories.org/about-the-pegasus-project/

Utopía Pirata

2026 – Partido Interdimensional Pirata

https://utopia.partidopirata.com.ar



partido
interdimensional
pirata

FUNDACIÓN
ROSA
LUXEMBURGO