GUIA RÁPIDA DE SEGURIDAD DIGITAL PARA ACTIVISTAS FEMINISTAS Y MUJERES EN RESISTENCIA

www.infoabortochile.org Linea Aborto Libre

GUÍA DE SEGURIDAD DIGITAL Y HOLÍSTICA PARA

ACTIVISTAS FEMINISTAS Y MUJERES EN RESISTENCIA

Esta guía fue desarrollada gracias a los conocimientos adquiridos en forma individual y colectiva por mujeres de distintos territorios y que como Línea Aborto Libre hemos implementado en nuestras prácticas.
Es parte de un trabajo conjunto que de forma autogestionada se ha organizado y hoy compartimos en base a las experiencias.

Para las mujeres que luchan, defensoras de los DDHH, de la tierra, es importante reconocer que es su derecho existir digitalmente de forma segura a través de estrategias, herramientas y elaboración de protocolos de seguridad que las ayudena tomar conciencia y control de su vida digital, mitigando riesgos tanto de amenaza como ataques directo de detractores de sus actuancias de lucha.

Esperamos se puedan incorporar conceptos básicos en seguridad digital aportando en la concientización del uso de internet y la seguridad de los datos con nuevas herramientas de protección de la información, para poder elaborar planes de acción frente a la protección de información sensible tanto individuales como colectivos.

Esta guía no cuenta con derechos de autoría y se permite su reproducción total por las vías que cuente o estime conveniente.
Confiamos en que este documento pueda ser un aporte a nuestros activismos y que nos proponga tomar conciencia de nuestra existencia digital, con herramientas certeras.

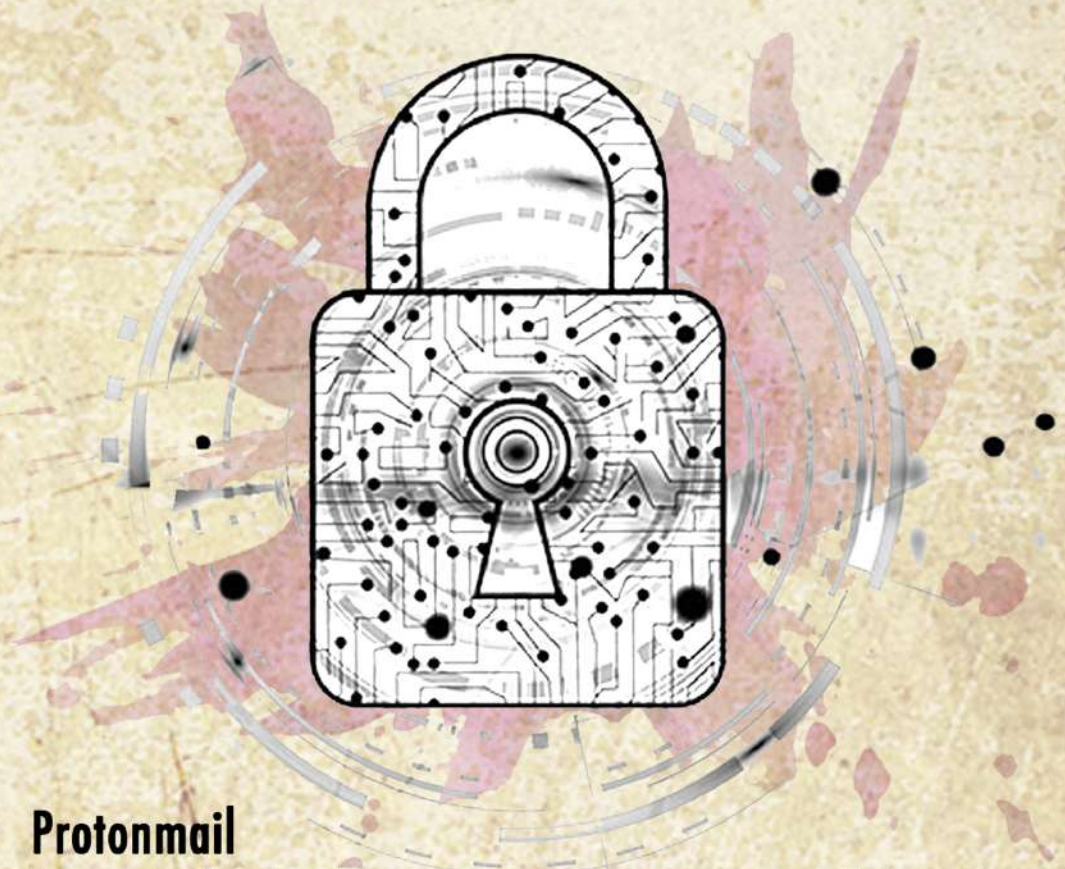
MAIL SEGURO ¿Por qué tener un mail seguro?

Las cuentas que se nos ofrecen desde plataformas como Google, Gmail, poseen conexión directa con el resto de aplicaciones de Google, por lo que nuestra información y las palabras que utilizamos se convierten en algoritmos que sirven para poder identificar nuestra actividad. Para esto, existen alternativas que nos permiten encriptar y anonimizar la información que enviamos.

Creación de un mail seguro:

Tenemos dos opciones, mail de Riseup o Protonmail.

En el caso de **riseup** debe recibir invitación la cual se obtiene a través de https://account.riseup.net/ ahí, quien ya cuenta con un mail, debe solicitar un código de invitación. Una vez se obtiene el código, el cual servirá para la creación de un solo mail, se debe ingresar en www.riseup.net e ingresar en solicitar una cuenta. Se sugiere crear cuenta con nombre distinto al propio y que la clave posea Mayúsculas, minúsculas, símbolos y números:
Por último, es muy importante guardar el código de verificación, ya que será solicitado si olvidas tu contraseña. Para realizar cifrado de mail con Riseup se requiere instalar Thunderbird, servicio perteneciente a Mozilla Firefox y que permite la organización de una o más cuentas. Para lograr el encriptado se debe incorporar complemento "Enigmail" tal y como se instalan los complementos en Mozilla Firefox. Una vez incorporado Enigmail se solicitara la creación de una "llave privada" la cual permitirá el acceso al mail encriptado. La llave pública es generada de forma automática y se puede compartir libremente para así recibir los mails cifrados de forma correcta



Protonmail

Para realizar la solicitud de mail en Protonmail no se requiere de invitación y se puede solicitar directamente en www.protonmail.com En este mail no se requiere realizar ninguna acción adicional para el encriptado de la información. Se sugiere iniciar sesión siempre desde Tor.

COMPUTADORES

Sistemas operativos: ¿qué es un sistema operativo?

Un sistema operativo es el principal software o conjunto de programas de un sistema informático que gestiona los recursos y provee los servicios a los programas de aplicación, es decir, administra los recursos del computador, coordina y organiza. Los principales sistemas operadores sin Window, IOS de Mac y Linux.

WINDOWS: Es el sistema operativo más usado, pertenece a Microsoft. Su Política de privacidad explica cuáles son los datos personales que recopilan, cómo los trata y con qué fines lo hace. Principalmente desde Windows 10 donde se declara que "Si elige no facilitar los datos requeridos para proporcionarle un producto o una función, no podrá usar dicho producto o dicha función. De igual modo, cuando necesitemos recopilar datos personales por imperativo legal, para celebrar un contrato con usted o cumplirlo y no facilite los datos, no podremos celebrar el contrato; o bien, si esto está relacionado con un producto existente que esté usando, puede que debamos suspenderlo o cancelarlo"

IOS: Pertenece a Apple, su política de privacidad indica que: "No estás obligado a facilitar la información personal que te soliciten, pero, si decides no hacerlo, habrá muchas ocasiones en las que no podrás utilizar los productos ni servicios, o no recibirás respuestas a las preguntas que pudieras tener".

LINUX: Por su parte, el sistema operativo Linux o su variación Ubuntu (basada en Debian) distribuido bajo una licencia libre o código abierto lo que significa que se basa en la colaboración y el libre acceso al código de fuente. Cuenta también con una variedad de aplicaciones gratuitas y de código abierto.

TAILS: Es un sistema operativo portátil basado en Linux y diseñado específicamente para la privacidad personal. Lo puedes instalar en un DVD o un USB, y usarlo para iniciar con ese sistema operático desde cualquier computadora, sea de Windows, Apple, o Linux. Tails es un sistema amnesiaco. ¿Qué significa esto? Significa que no guardad ningún dato entre cada sesión. Cada vez que lo usas, empieza de cero un espacio digital nuevo, sin información personal que te pueda identificar, sin importar que computadora usas, ni de quién es. Todas las conexiones de internet pasan por la Red Tor, entonces tu dirección de IP, ubicación, y actividad no se pueden vigilar fácilmente por terceras

INDICACIONES BÁSICAS EN EL USO DE INTERNET

Tener prácticas seguras en internet no es solo es instalar y usar las aplicaciones seguras sino también tener ciertos hábitos que podrían mejorar nuestra experiencia y evitarnos malos ratos. Acá mencionaremos algunas situaciones donde nuestra información podría ser expuesta o filtrada por lo que es importante de considerar.

No entres a sitios web desde un link en un email.
Como regla general, si un email te lleva directo a una pantalla de acceso, deberías sospechar. Es mejor ir directamente al sitio desde el navegador, acceder normalmente, y buscar la página que el mail te sugería. Una excepción a la regla es cuando has pedido cambiar tu contraseña para un sitio en particular.

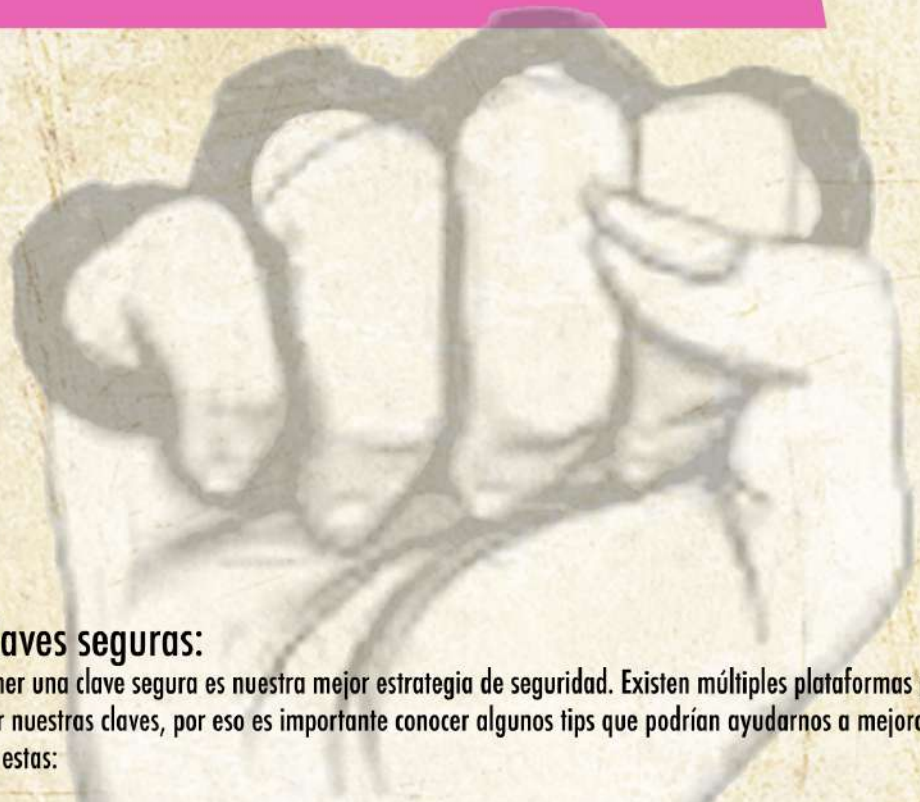
Evita usar Facebook, Twitter o Google para acceder a otros sitios
Muchos sitios ofrecen la oportunidad de acceder con tu cuenta de red social, en vez de tener que registrarte con el sitio de cero. Aunque parece conveniente, en realidad presenta un gran riego a tu seguridad virtual: ¿cómo sabes que el sitio es legítimo? Es mucho más seguro crear una nueva cuenta para el sitio. Al alentarte para acceder con una cuenta de red social, un sitio malintencionado puede fácilmente recolectar información valiosa como nombres de usuario y contraseñas

No confíes en emails que piden tu información privada

Datos de encuestas o lo que sea que pueda revelar información sobre tu persona, sin importar lo profesional que parezcan.
La mayoría de los sitios web no necesitan de tus datos personales para proveerte sus servicios, por lo cual puedes sospechar si te los piden

WIFI público

Cuando estas usando una red de wi-fi sin contraseñas o público, cualquier persona compartiendo la misma red puede interferir tu tráfico o mirar tu actividad



Claves seguras:

Tener una clave segura es nuestra mejor estrategia de seguridad. Existen múltiples plataformas para poder obtener nuestras claves, por eso es importante conocer algunos tips que podrían ayudarnos a mejorar la elaboración de estas:

*Lo primero es crearlas en base a una mezcla aleatoria de letras, números y caracteres especiales es lo mejor. Cuanto más largas, mejor. Intenta usar más de 12 caracteres siempre. Un buen ejemplo de esto es quizás alguna frase que recordemos fácilmente, como la de una canción, poema o libro.

*Existen plataformas o páginas que no permiten contraseñas tan largas, como por ejemplo las de los bancos, en ese caso quizás elegir sólo una palabra y mezclar con números y símbolos.

*Sí vas a usar palabras reales en tu contraseña, trata de usar palabras y referencias poco conocidas o mal escritas. Palabras de diccionario o de cultura popular no son una buena idea. Por ejemplo, si quisiera poner el nombre de una ciudad, elegir su abreviación: en lugar de Santiago, solo Stgo.

*Además, es muy importante no repetir la misma clave para todos mis accesos. Para eso existen aplicaciones llamadas "llaveros" donde sólo debemos recordar una sola clave y la app hace lo suyo.

NAVEGADORES

El navegador más usado, tanto en los sistemas operativos Windows como IOS es Google Chrome. Este es parte de Google.
Posee sincronización con motor de búsqueda Google, ubicación, YouTube, Play Store, Gmail, calendario, drive, traductor, sincronización de fotos entre otros.
Teléfonos Android vienen con este sistema operativo por defecto, por lo que la sincronización es automática.
En el caso de los computadores podemos minimizar la información por medio del cierre de sesión del usuario google, el cual se activa de forma inmediata una vez se inicia sesión de Gmail.
Este navegador se recomienda solo para el uso de actividades que no impliquen medidas de seguridad o cuando existen páginas a las que sólo se puede acceder o se posee una mejor experiencia. (Por ejemplo, si queremos ver una película on line)
Mozilla Firefox y complementos: Mozilla Firefox en su política de privacidad indica su compromiso en la mínima recopilación de datos de sus usuarios en sus navegaciones. Además pone a disposición complementos, los cuales son como APPS o pequeños software para el navegador y que permiten mejorar la seguridad, rendimiento y funcionalidad. Los complementos de Mozilla Firefox son de fácil instalación en el mismo navegador.

Complementos para instalar:

DUCKDUCKGO: es un motor de búsqueda, al igual que Google, pero, protege tus datos mientras busca y navega: bloqueo de rastreadores, cifrado más inteligente, búsqueda privada y más.
HTTPS Everywhere: ¡Cifra la web! HTTPS Everywhere es una extensión para proteger tus comunicaciones al habilitar el cifrado HTTPS automáticamente en las web que lo soportan, incluso cuando escribes URLs o sigues vínculos que omiten el prefijo "https:".
GHOSTERY: Bloqueador de anuncios para privacidad. Bloquea anuncios, detiene rastreadores y acelera sitios web.
PRIVACY BADGER: Aprende automáticamente a bloquear rastreadores invisibles. En lugar de mantener listas de qué bloquear, Privacy Badger descubre automáticamente los rastreadores mientras navega por la Web. El rastreo invisible ocurre de muchas maneras; los anuncios son solo la punta visible del iceberg. Privacy Badger envía la señal No rastrear a los rastreadores diciéndoles que no le rastreen. Si ignoran sus deseos, Badger aprende a bloquearlos, ya sean anunciantes o rastreadores de otros tipos.
FACEBOOK CONTAINER: Impide que Facebook siga tus movimientos por la web. La extensión Facebook Container para Firefox te ayuda a tomar el control y aislar tu actividad en la red para que Facebook no pueda verla.
ADBLOCKER ULTIMATE: Bloqueador de anuncios gratuito y mejorado. Eliminar completamente TODOS los anuncios. ¡Sin anuncios "aceptables" o anunciantes en la lista blanca, bloqueo de seguimiento, bloqueo de malware!
Disconnect: Visualiza y bloquea los sitios web invisibles que rastrean su búsqueda y su historial de navegación.

Los **VPN** son extensiones de una red privada, para que cuando generamos tráfico de datos, este viaje de forma cifrada.
Una VPN crea una conexión privada, cifrada, entre tu computadora y un servidor de VPN: toda tu actividad de internet se "filtra" a través de esta red antes de salir del servidor de VPN al mundo. Cuando accedes un sitio web a través de la conexión VPN, el sitio percibe el pedido de datos desde el servidor de VPN, y no desde tu computadora. Alguien queriendo intervenir lo que va desde tu computadora al servidor VPN no puede ver lo que haces, ya que todo está cifrado. Es como un túnel secreto entre tu computadora y el servidor VPN. El servidor saca al mundo lo que le das (y recibe lo que le pides), a través del túnel secreto, pero nadie puede ver lo que está adentro del túnel
TunnelBear VPN: También se puede instalar desde complementos de Mozilla Firefox.

PROYECTO TOR es un navegador que permite privacidad y libertad sin rastreo, vigilancia o censura. Tor Browser aísla cada sitio web que visitas para que los rastreadores y anuncios de terceros no puedan seguirte. Cualquier cookie se borra automáticamente cuando termina de navegar. También lo hará su historial de navegación. Tor lo que realiza es la utilización de distintas direcciones IP a través del mundo y así poder anonimizar tu navegación. El proyecto Tor promueve los derechos humanos y defienden nuestra privacidad en línea a través de software libre y redes abiertas Este navegador se instala directamente desde la página https://www.torproject.org/

No se recomienda para uso de redes sociales o uso de mail como por ejemplo Gmail. También es MUY IMPORTANTE NO MAXIMIZAR LA PÁGINA, YA QUE SE PIERDE PRIVACIDAD. Usémosla en el tamaño en que este se nos presenta.

CELULARES

En el caso de los celulares tenemos las opciones de Android y IOS. Es importante recordar que en nuestros teléfonos mantenemos una gran cantidad de información personal, es por esto que es importante mantener al día las actualizaciones de las aplicaciones que utilizamos, así como mantener un control de los permisos que otorgamos a cada una de estas. Una forma importante de disminuir al máximo los metadatos de nuestros equipos es desactivando la ubicación.
Es importante, para ambos sistemas operativos, saber que al momento de utilizar las apps seguras para realizar videollamadas o envío de audios, desactivar el micrófono para el resto de las aplicaciones. Se recomienda solo el envío de mensajes escritos.

SIGNAL: Signal es una app de envío y recepción de mensajería, videollamadas y llamadas telefónicas. Puede ser descargada tanto desde app store como Google Play. Signal posee un protocolo de cifrado de código abierto integrado, creado por desarrolladores libres sin publicidad ni rastreadores.

Es importante enviar fotos o videos capturados directamente desde la App para que estos no adjunten los metadatos de los celulares (marca del teléfono, fecha y ubicación).
Por último, y esto se recomienda para cualquier aplicación donde se guarde información, es nuestra responsabilidad ir eliminando los chat. Signal tiene la posibilidad de agregar una cantidad de tiempo –Desde un par de horas a días- para la desaparición automática de los mensajes. Signal se encuentra disponible también para su utilización web, es decir, desde un computador. Se recomienda utilizar Mozilla Firefox o Tor.
WIRE: Al igual que Signal, Wire permite el envío y recepción de mensajería, videollamas y llamada de forma segura y con cifrado integral. No posee código abierto y al igual que Signal puede ser descargado directamente desde App Store o Google Play
JITSI MEET: Es una App para realizar videollamadas cifradas, disponible tanto para celulares –IOS o Android- como para computadores. Puedes instalar la aplicación en el celular o a través de un link http://meet.jit.si y lo único que se necesita es la autorización del micrófono y la cámara. Para crear la videollamada se debe crear una sala, la cual además se puede crear una contraseña para ingresar y una vez dentro se puede literalmente "cerrar" la conversación por medio de un simple click en un candado. Además, la videollamada por Jitsi puede ser entre dos o más integrantes, siendo un instrumento fundamental para reuniones a distancia.
VPN: Tal y como para los computadores, un VPN en el celular es fundamental para mantener la privacidad de nuestro celular, al igual que para el computador podemos instalar Tunnelbear por medio de Google Play o App Store y podemos seleccionar el país donde queremos se ubique nuestra IP.

NO QUIERO TU PERMISO
POR ESO ABORTO
CON LAS TORTAS Y CON MISO.