MANTÉN LA CALMA Y DEFIENDE EL TERRITORIO DIGITAL

Tips de cuidados digitales en tiempos de pandemia

******

INICIATIVA MESOAMERICANA de mujeres defensoras DE DERECHOS HUMANOS

¿Cómo proteger nuestro territorio digital en tiempos de COVID19?

Ante la crisis sanitaria las defensoras de Derechos Humanos reinventamos el espacio digital en este presente nuestro territorio de lucha y resistencia. Y en este accionar los cuidados digitales desde una perspectiva feminista son clave para poder establecer una comunicación virtual segura. Con esta guía queremos compartir algunos consejos y orientaciones para nuestro uso cotidiano del ciberespacio.

Te acercamos este fanzine para entrar en detalle de los riesgos que existen en el mundo virtual y así cuidar nuestras huellas digitales y conocer aquellas prácticas que nos vulneran en nuestra labor como defensoras. Hoy es vital la colectivización de saberes para ayudarnos a proteger nuestras experiencias en línea y para que construyamos juntas una internet feminista.

Estamos haciendo un gran esfuerzo por trabajar de forma virtual. Seguimos siendo corporalidades inquietas y movedizas, solo que ahora nos resulta fundamental nuestro acceso a internet. Muchas veces nuestras posibilidades se ven limitadas, vivimos la sobrecarga del trabajo de cuidados y trabajamos en espacios reducidos. Por eso también recomendamos algunos cuidados para que tu corporalidad recuerde que necesita cuidados para poder estar bien en este espacio.

Antes que nada: mantén la calma. Aquí unos cuidados para la vida fuera de la pantalla:

- Elonga: estira y rota tus hombros con conciencia varias veces al día. Estira las muñecas y los codos, levántate cada 30 minutos.
- Bebe suficiente agua: mantente hidratada
- Cuida los ojos: fija la vista en puntos lejanos, parpadea seguido (evita el síndrome del "ojo seco").
- Mira por la ventana o levántate a dar unos pasos: limita tus horas en la pantalla y toma descansos cada 2 horas.

****

ATAQUES Y MEDIDAS A TOMAR QUE TENEMOS A MANO

Como Defensoras de Derechos Humanos enfrentamos diferentes agresiones a raíz de nuestra labor. En nuestro territorio digital esta violencia no es menor. **El control y la vigilancia en el ámbito digital es cada vez mayor hacia nosotras, nuestras comunidades, organizaciones y movimientos.**
Compartimos unas medidas concretas, a la mano, y fundamentales para cuidar nuestra identidad y territorio digital.

CONOCE EL ATAQUE MÁS POPULAR DE ESTA PANDEMIA...EL PHISHING:

¿Qué es exactamente el phishing?

Es un tipo de ataque informático que se estuvo multiplicando durante la pandemia.

¿FISHING? ¿Tiene que ver con pescar en idioma inglés? Phishing con P. Es parecido y tiene que ver con pescar. Vamos a ver cómo evitar el robo de datos, contraseñas y cuentas.

El phishing es una de las estafas más antiguas y mejor conocidas de internet. Podemos definirlo como un tipo de fraude digital que emplea trucos de ingeniería social para obtener datos privados de tus comunicaciones.

Una vez obtenidos nuestros datos, pueden suplantar nuestra identidad en nuestras cuentas de internet para:

- extorsionarnos
- adueñarse de nuestra audiencia y seguidorxs
- robarnos dinero (en el caso de fraudes a cuentas bancarias)
- publicar por nosotras

Te daremos algunos tips a seguir para prevenir caer en un fraude de phishing

Primero respira profundo y mantén la calma pero si te piden usuaria, contraseña y otros datos sensibles mediante algún mensaje que parece urgente o algún formulario, inclusive si viene de la cuenta de una persona conocida, no actúes de manera inmediata.

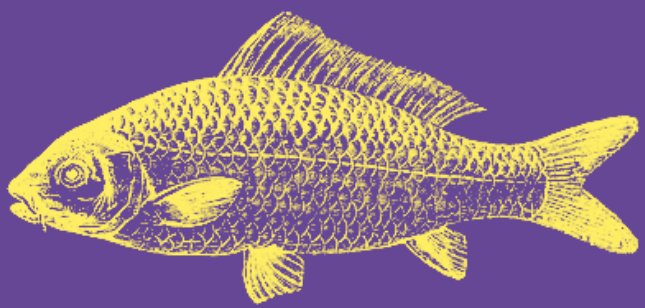
Una de las técnicas de engaño que más se repitieron durante el Covid19 fue la de pedir a perfiles que comparten textos o imágenes una comprobación de que no restringen el derecho de autor. Otra trampa es solicitar que la cuenta es tuya cualquier día, sin aviso previo y por medio de otra plataforma (por ejemplo: que te contacten por Whatsapp haciéndose pasar por el "equipo de Instagram"). Por último, otra forma común de engaño es abrir o descargar archivos adjuntos que no esperabas- Y si al final de la jornada siguen insistiendo con tus datos sensibles, **NO LOS COMPARTAS AMIGA**. Considera que estas informaciones son equivalentes a las llaves que abren la puerta de tu casa, por eso bajo ningún concepto debes compartir esta información con terceros/as.

* ¡Atención! Cuando interactuamos en redes sociales nunca podemos saber a ciencia cierta la identidad de quien nos habla (más cuando no conocemos al remitente).

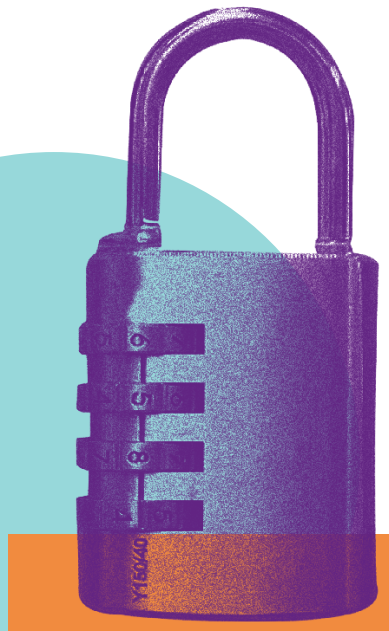
* Activa la sabia sospecha: si algún mensaje o propuesta te parece dudosa contacta por otro medio a quien te escribe o, directamente, no respondas.

* También atestiguamos que los ataques en la plataforma Zoom (conocidos como "Zoom bombing") arreciaron durante la pandemia. Para prevenirlos te recomendamos nuestra guía:

Guía fácil para comunicarnos (y conspirar) en espacios seguros durante COVID-19
(http://im-defensoras.org/2020/06/guia-facil-para-comunicarnos-y-conspirar-en-espacios-seguros-durante-covid-19/)



QUÉ HACER PARA PROTEGER MI IDENTIDAD DIGITAL



CONTRASEÑAS SEGURAS:

Las contraseñas que le pongas a tus aplicaciones, cuentas y dispositivos son las llaves de acceso a tus fotos, mensajes, contactos, es decir: a toda tu información. Debido a que son la primera y muchas veces única defensa para acceder a tus cuentas, las contraseñas potentes son fundamentales.
Compartimos unas reglas generales para crear buenas y fuertes contraseñas:

Una contraseña se considera segura cuando:

* Es extensa y contiene más de 13 caracteres.
* Entre esos caracteres es aconsejable mezclar mayúsculas, minúsculas, símbolos y números.
* Es privada: no la compartes con nadie.
* Es única: no repites la misma contraseña en más de una cuenta.
* Parecida al cepillo de dientes: la cambias con regularidad.

Con todos estos tips seguramente te preguntes, cómo hacer para recordarlas. Existen las billeteras o llaveros para contraseñas. Por eso, si crees que la memoria puede fallarte, descarga **KeepassXC** https://keepassxc.org/ o cualquier llavero seguro como **Bitwarden** https://bitwarden.com/. Estos llaveros te ayudan a guardar cada contraseña compleja en un lugar diferente y solo debes recordar **UNA SOLA CONTRASEÑA** maestra para usar todas las demás.

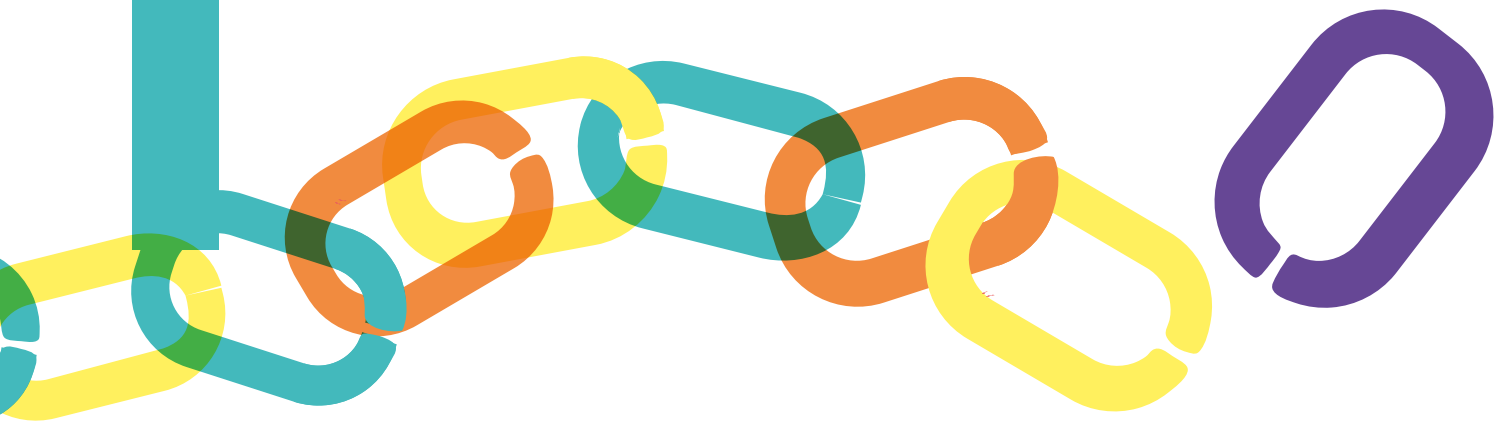
REVISA LAS APLICACIONES LIGADAS A TUS CUENTAS:

Muchas usamos nuestros perfiles de redes para acceder a diferentes servicios de internet, o los damos de alta en otras páginas y aplicaciones para poder compartir con otras personas nuestros intereses o utilizar servicios complementarios.

Es decir que cada aplicación que instalamos una vez y hace tiempo tiene, a su vez, ciertos permisos para acceder a información de nuestro celular o de nuestras cuentas en la Web.

Te recomendamos que en las Configuraciones de tu teléfono, busca la sección Aplicaciones y revisa los permisos de acceso a tus archivos. Observa si realmente los necesita, si la respuesta es no: intenta anular ese permiso. Por ejemplo: Instagram pide permiso para usar nuestro teléfono, contactos y ubicación. **Si realmente no los necesitas ¡desactívalos!**

También puedes hacerlo desde una computadora: revisa cada plataforma y cuáles son los accesos que le otorgaste ¿siguen activos? Piensa si quieres que siga así o puedes darle de baja.
Una buena medida para las aplicaciones que sigues usando, especialmente en tu celular, es actualizarlas asiduamente.



ASEGURA TUS PERFILES EN REDES SOCIALES

Ante la crisis que atravesamos llegó la hora de reflexionar profundo y en calma:

¿Qué quieres compartir con les otres? ¿Cuánto de tu vida personal quieres mostrar?

Las redes sociales son redes humanas y, por eso, debemos cuidarlas. Seamos meticulosas con la información que compartimos en estos espacios. Manejar esa información de manera estratégica significa pensar qué queremos alcanzar en ese espacio y, por tanto, cuál es la información útil y necesaria para nuestro objetivo en esa red.

Las configuraciones que tenemos en redes sociales como Twitter, Facebook, Instagram, TikTok, entre otras, deben ser re-pensadas a la luz de la importancia de nuestra privacidad que permite el pensamiento crítico y disidente. Por eso te recomendamos:

* Revisa en configuración de privacidad con quién compartes tus posts: ¿A quiénes quieres ser accesible como contacto? ¿ Quiénes quieres que vea, comparta y etiquete tu información?
* Consulta el consentimiento de las personas sobre las que publicas imágenes, videos y otros materiales. ¡No lo des por sentado! Así como tampoco permitas que se publiquen imagenes tuyas sin tu consentimiento.
* Limita el público de tus publicaciones anteriores: borra contenido personal que puede ponerte en riesgo (ubicación de tu casa, de tus familiares, rutas que tomas, etc.)
* Activa la verificación de 2 pasos: protege de esta manera el ingreso a nuestras cuentas.
* En caso de recibir ataques: registra, revisa la información disponible sobre la o las personas agresoras que está disponible en línea, haz capturas de pantalla de todo lo que sea posible (en caso de que esta información sea removida posteriormente) y denuncia.

Puedes ponerte en contacto con nosotras a comunicacion@im-defensoras.org

RESPALDA LA INFORMACIÓN DE TU DISPOSITIVO:

Todos los días creamos información, compartimos fotos, documentos videos y/o audios que son preciados para nuestros recorridos biográficos y también profesionales. **Pero la tecnología puede fallar, ¡de hecho sucede tan seguido!, y de un día para el otro podemos perder nuestros documentos. Una forma de salvaguardar nuestra preciada información es ¡respaldar!**

Un respaldo no tiene que ser algo complejo, realmente debe cumplir unas reglas básicas:

- Debe estar lo más actualizado posible, de preferencia no mayor a un mes
- Debes respaldar lo más valioso o indispensable que consideres dentro de universo de archivos en tu computadora o celular.
- Un respaldo es una copia de información, por lo tanto no es para uso diario de consulta.
- Mantén el dispositivo de almacenamiento en un lugar seguro de robo o percances (agua, temperaturas variables, caídas o mal uso).

Es simple llevar un orden y mucho más en tu computadora. Para hacerlo sencillo sigue estos consejos:

- Descarta todos esos archivos que están en esa carpeta descargas y nunca volviste a consultar.
- Limpia un poco tu escritorio y comienza a colocar tus archivos en carpetas que puedas identificar fácilmente.
- Los archivos duplicados pueden ocupar mucho del espacio de tu disco duro y estorbar cuando hagas el respaldo.
- Separa bien tus archivos: además de hacer tu vida más sencilla, te permitirá tener bien organizados tus documentos de trabajo, lejos de tu información personal.

¿Cómo haces un respaldo? Hay varios programas que te permiten hacerlo rápido de manera automatizada, casi sin que te des cuenta. También puedes hacerlos manualmente y reservar en tu agenda un Lunes o un Viernes de "respaldo party" :-).

ACTIVA LA VERIFICACIÓN DE 2 PASOS:

La verificación de dos pasos o doble autenticación añade una capa de seguridad a las cuentas de redes sociales, correo electrónico y mensajería instantánea. Se puede activar en: Gmail, Hotmail, Yahoo, Facebook, Twitter y Whatsapp, Instagram, Telegram, Wire y generalmente está vinculada a tu teléfono, enviándote un código temporal como una segunda contraseña. También puede estar vinculada a un correo electrónico.

Activa la verificación de dos pasos en tus cuentas siguiendo estos pasos (cambian un poco dependiendo de cada servicio):

* Busca la sección de configuración de tu servicio.
* Busca la opción de seguridad o privacidad.
* En la sección de privacidad deberás encontrar una opción que diga **activar verificación de dos pasos.**
* En muchos de los casos te solicita un número telefónico para activar la verificación.
* Escanea el código QR con tu aplicación para activar un número aleatorio de seis dígitos.
* Existen opciones de configurar un segundo correo electrónico de respaldo para cualquier cuenta o servicio.
* Revisa las opciones disponibles ¡son de gran ayuda!

CUIDANDO A NUESTRAS MASCOTAS (MEDIDAS PARA CELULARES)

CIFRA TU TELÉFONO CELULAR

El cifrado nos ayuda a poner la información en algo parecido a una caja fuerte. Nos recuerda también a los jeroglíficos o a los juegos secretos de la niñez en los que escribíamos cartas con tinta invisible, la famosa "tinta limón" que solía leerse a contraluz.
Cuando trabajamos con información sensible, asegurar nuestros datos y cuidar a nuestras compañeras es clave. Para Android, desde la versión 4.0 hasta la última versión, puedes encender encriptar (o cifrar) el dispositivo. Para ello ve a:

- Configuración
- Seguridad
- Encriptación

Es importante mencionar que para equipos IOS el cifrado es generado por defecto.
Antes de que puedas utilizar la configuración para encriptar el dispositivo, tendrás que activar una contraseña de bloqueo de pantalla. Es recomendable utilizar una contraseña segura o PIN en lugar del desbloqueo por patrón.

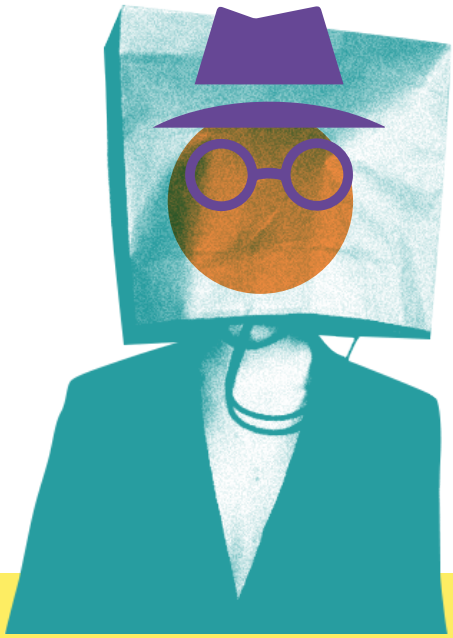
Un buen consejo: antes de iniciar el proceso de cifrado, asegúrate que tu teléfono esté preferentemente conectado a la electricidad y que tengas una copia de seguridad de tus archivos.

DESACTIVA LA GEOLOCALIZACION O GPS:

Revisa desde la configuración de tu celular cuáles son las aplicaciones que tienen acceso a tu ubicación, ya que es posible activar y desactivar esta opción y usarla únicamente cuando la necesites. Hazte la pregunta: **¿realmente necesitas estar geolocalizada en todo momento?**

Es importante que estos servicios no estén activados de manera predeterminada pues si lo están aumentan el riesgo de rastreo de tu ubicación, consumen más rápido la batería y alimentan el flujo de datos no deseados que inician aplicaciones que se ejecutan de manera secundaria o que tu operador móvil ejecuta de manera remota.

NAVEGA LIBRE Y USA EL ANONIMATO A TU FAVOR



CONSIDERA LA NAVEGACIÓN ANÓNIMA

Así como las huellas en la playa hablan de la presencia humana, cada acción nuestra en internet deja una marca.

¿Ya lo sabías? Absolutamente todo lo que hacemos en la Red imprime una huella, es registrado o analizado por alguien a posteriori.

Los navegadores más usados como Firefox o Chrome no ocultan la huella de la que hablamos al principio, entonces debes tener en cuenta que cualquier sitio, hacker mal intencionado, o gobierno pueden conocer tu ubicación física y los sitios que visitas al registrar el histórico de los datos que tu computadora envía y recibe (aunque no puedan acceder al contenido). En el caso del gobierno, o de un proveedor de internet, en casos de censura más o menos extrema pueden bloquear el acceso a ciertos sitios. Los navegadores más usados nos exponen a estos peligros, sin importar las extensiones de seguridad que instales.

Si estás en una situación en la cual necesitas ser anónima, por razones de seguridad o de actividad política, deberías usar la red Tor. Para poder utilizarla, lo único que tienes que hacer es bajar el Navegador Tor y usarlo de la misma manera en que navegas con Firefox o Chrome. Lo único que puede llegar a molestar es que la red Tor es más lenta que la normal: tarda unos segundos para mandar tus pedidos de datos a través del mundo.

Puedes bajar TOR en https://www.torproject.org/es/ y comenzar a navegar con privacidad. Defiendete de la vigilancia de red y el análisis de tráfico. Elude la censura.

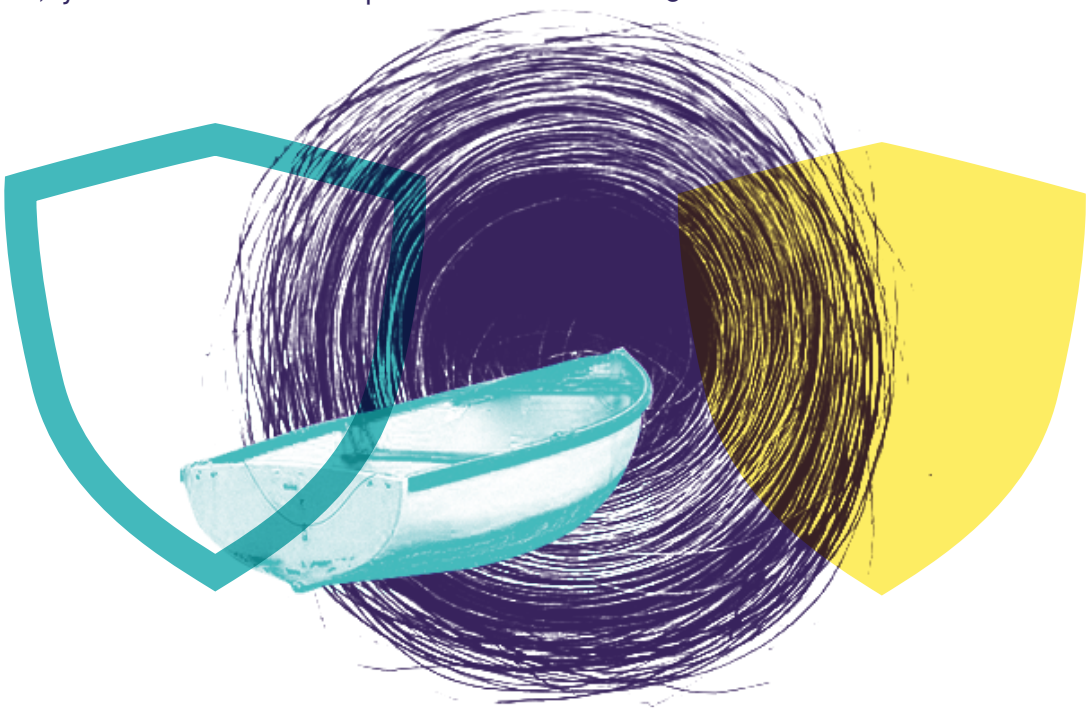
VAMOS A NAVEGAR CON VPN PERO ¿DE QUÉ SE TRATA?

Ser Defensoras teniendo en cuenta la sensibilidad de nuestra labor nos exige hacer un cambio: posicionarnos desde una actitud mas preventiva. Por eso necesitamos informarnos y saber qué servicios están disponibles para protegernos. Por eso necesitamos hablar de....¡VPNs!

¿Qué es? Una VPN (en inglés: Virtual Private Network) es una forma de conectar a internet a través de la creación de una conexión privada, cifrada, entre tu computadora y un servidor de VPN: esto significa que **toda tu actividad de internet se "oculta" por medio 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. Si alguien quisiera intervenir lo que va desde tu computadora al servidor VPN no podría observar lo que hacés, ya que todo está cifrado (lo que significa: que la información viaja cerrada en sobres sellados).

Imaginate que se abre un túnel secreto entre tu computadora y el servidor VPN. Lo más interesante es que hay servidores VPN en casi todo el mundo, por eso si el servidor que utilizás está en Suecia, los sitios que visitas registrarán que eres sueca, porque las solicitudes las recibirán desde el servidor en Suecia. Igualmente, si usas un servidor en Malasia los sitios pensaran que eres de ese país. Mientras tanto los intermediarios de tráfico (empresas que te proveen el servicio de internet o espías que responden a gobiernos) no podrán detectar la huella de tu navegación.



Algunas VPN que puedes explorar son:

NordVPN

NordVPN es un servicio VPN pago, enfocado en ofrecer un servicio de alto rendimiento en el cual no haya perdida de velocidad. Cuenta con clientes para Windows, Mac OS, Android y iOS, así como complementos para Firefox y Chrome, pudiendo con una sola cuenta configurar hasta 6 dispositivos diferentes. https://nordvpn.com/

ProtonVPN

ProtonVPN es un proyecto con enfoque de privacidad en línea para proteger a los activistas y periodistas del mundo junto con ProtonMail.
Actualmente el servicio se ofrece a través de más de 100 servidores en más de 14 países del mundo. Cuenta con clientes para GNU/Linux, Mac OS, Windows, Android y iOS, y se puede encontrar de manera freemium (planes gratuitos y de paga). https://protonvpn.com/

TunnelBear

TunnelBear es un servicio de VPN freemium con cliente multiplataforma para equipos de computo (GNU/Linux, Mac OS y Windows), móviles (Android y iOS) y navegadores web (Google Chrome y Opera).
El servicio de TunnelBear ofrece la posibilidad de conectarte a más de 20 países diferentes. Tiene versiones gratuitas y de pago.https://www.tunnelbear.com/

******

Fuentes consultadas para realizar esta guía:

socialtic.org/
protege.la/
latfem.org/kit-de-cuidados-digitales-para-periodistas-feministas/
y Red de periodistas feministas de Latinoamérica y el Caribe.

INICIATIVA MESOAMERICANA de mujeres defensoras DE DERECHOS HUMANOS

Diseño gráfico
La Propia Agencia