Manual de seguridad digital:

kit de herramientas para una internet feminista

Larissa Saud
[trayectos.org]

Índice

Introducción

Se asume generalizadamente que la privacidad en internet no existe. Pero el ver cotidianamente cuestionamientos sobre la identidad de género o la sexualidad, siendo objetos de acoso *off-line* y *online*, hace importante reanudar el debate sobre la privacidad en internet. Muchas veces estos ataques se aprovechan de la abundancia de datos que dejamos con nuestra "huella digital".[1]

Las huellas digitales son rastros, datos que existen acerca de ti, una especie de "sombra digital" que creamos y a la cual vamos agregando más datos cuando usamos herramientas, aplicaciones, navegadores y variados servicios digitales. Los rastros digitales son creados por ti y también por otras personas al publicar informaciones. Todo ello incluye lo que escribes, publicas y compartes, así como el contenido que otras personas crean acerca tuyo cuando te etiquetan en fotos, te mencionan en tuits o simplemente se comunican contigo a través de un correo electrónico o una sesión de chat.

Pero... ¿por qué un manual con una perspectiva de género?

La violencia que viven las mujeres en territorio *online* es completamente diferente de la que sufren los hombres. No es casualidad que seamos la mayoría de las víctimas cuando se trata de crímenes cibernéticos.

Distinta también es la violencia y la discriminación que sufre la comunidad LGBTQ. El Safe Hub Collective lo resume así:

> «Los peligros a la autonomía digital son de género, raciales, queerfóbicos, transfóbicos y clasistas por naturaleza. La severidad de estos peligros tiene repercusiones físicas y psicológicas profundas para aquellos que las experimentan: no se pueden tomar a la ligera».[2]

Si en el día a día, nosotras, feministas, luchamos para que nuestros cuerpos no sean objeto de asedio, violación, racismo, lesbiofobia, transfobia y criminalización, ¿qué pasa en el medio virtual? ¿Damos nuestros datos a los *chupadatos*? ¿Nuestro período menstrual para las *app*, sin saber a dónde va parar?[3] ¿Un *nude* almacenado en la nube de Whatsapp sin saber hasta cuándo?

Cuando damos a "Estoy de acuerdo" en muchas de las aplicaciones firmamos un contrato y con eso damos datos, fotos, contactos o ubicación a alguien que no sabemos quién es, dónde está ni qué va a hacer con esos datos.

¿Acostumbras a ir por ahí hablando de tus intimidades a desconocidos? Si usas *app* de Google Play como muchos mortales del siglo XXI, pues sí. Lo haces. Las políticas de privacidad son largas y confusas. Tendemos a simplemente hacer clic. Sin embargo, cuando entregamos nuestros contenidos personales a una empresa comercial, deberíamos saber qué les estamos permitiendo hacer con ese contenido. Si las letras pequeñas te agobian, en este enlace, en menos de 5 minutos, podrás conocer sobre las políticas de privacidad de las principales redes sociales actuales.

1 Manual *Zen y el arte de que la tecnología trabaje para ti*.

2 Jazmín Acuña (2017): "Buscando a las mujeres en el Plan Nacional de Ciberseguridad". 9 de mayo de 2017 en *TEDIC*.

3 Florencia Goldsman (2018): "Menstruapps o cómo hacer negocio con los datos íntimos de millones de mujeres". 24 de marzo de 2018 en *El Salto*.

Pero no pasa nada... No tienes nada que ocultar, ¿verdad?

Vamos a enumerar 7 motivos[4] que sabemos que vas usar para confiarte en que "no pasa nada".

1. **No tengo nada que esconder.** La privacidad no se trata de esconderse, sino de autonomía, poder y control.
2. **No me importa.** Cuando miras cuidadosamente las rastros digitales que creas, encontrarás una mezcla: algunas serán banales —tu desayuno—, pero otros pueden ser mucho más personales.
3. **Sólo es internet.** Internet te rodea y tus rastros digitales se han convertido en tu reputación.
4. **Pero sólo soy una persona entre millones, ¿cómo pueden verme?** Ser "una persona entre millones" no implica que puedas "esconderte en la multitud"; significa que cuando una máquina compara tus datos con los datos de las demás personas, es más fácil encontrar las atípicas.
5. **Pero me dan un descuento en el seguro.** Cuando vas a tu médico/a, tu comunicación está protegida. Esto está embebido en el concepto universal de la confidencialidad paciente-médico para asegurar que puedas expresarte libremente con tu médico/a sin estar preocupado/a de posibles repercusiones como el aumento de tu tasa de seguro.
6. **Pero me están brindando el servicio gratuitamente.** No es gratis: estás pagando con tus datos.
7. **No soy de Occidente, no me afecta.** La colección de datos es un asunto global. Prestamistas en países africanos, así como en EE. UU. se están basando en plataformas de redes sociales e historiales de teléfonos celulares para evaluar si alguien es susceptible o no de recibir un crédito.

Si todos estos motivos no te valen, vamos darte aglunos más: tenemos ejemplos todos los días de mujeres que son amenazadas por sus ex, por sus compañeros, por sus jefes y por otros hombres, donde fotos, datos y otras informaciones son expuestas, llevando la violencia *online* a extremas consecuencias en la vida real.

En el *off-line* estamos más acostumbradas a pensar en soluciones colectivas para nuestra organización y seguridad. Usar las redes sociales es estar atentas a los riesgos a los que estamos expuestas. La lucha y resistencia en internet parecen ser profundamente individualizadas, lo que torna a determinadas personas en objetivos fáciles de atacar.

4 Véase el proyecto "Yo y Mi sombra- Toma control sobre tus datos".

VAAAAALE... TODO MUY BIEN, ¿PERO POR DÓNDE EMPIEZO?

Antes de nada, respira. Este manual no pretende ser una chapa, ni dejarte más agobiada o preocupada creyendo que nada tiene solución.

Felizmente, hay ciertas propiedades físicas de la información que hacen que cifrar informaciones sea más fácil que descifrarlas. Los cambios de algunos hábitos y la utilización de criptografía y de *software* libre y de código abierto, pueden proporcionar un nivel bueno de privacidad, aunque no garantizan la seguridad total.

Además de *software* y *hardware*, también es importante tener una visión holística de la seguridad y por eso vamos hablar de estrategias de mitigación de manera general, antes de entrar precisamente en aplicaciones y *software*.

DINÁMICA PARA HACER A SOLAS

[Para concientización de acciones cotidianas y de la presencia de la tecnología en nuestras vidas]

– **Dibuja un día típico de tu vida.** Qué tecnologías utilizas, cuántas, en qué dispositivos. Desde que te despiertas hasta cuando comes y duermes:

¿Cuándo te levantas?
¿A dónde vas y cómo?
¿Qué llevas contigo?
¿Con quién estás y qué trabajo/actividades realizas?
Cuando terminas de estas actividades, ¿qué haces después?
¿Cuándo te relajas/duermes?

– **Analiza la sensibilidad y vulnerabilidad de estos datos...**

– **¿Qué quieres destacar de este análisis?**

– **¿Que pasaría si estos datos desaparecieran?:**

¿Tienes una copia? ¿Y donde está?
¿Qué pasaría si una persona a la que no hemos dado permiso accediera?
¿Estos datos son de información personal identificable —nombre, apellido, DNI/NIE, número de Seguridad Social—?
¿Son información sensible —orientación sexual, temas de salud, creencias religiosas, etc.—?

¿Qué es una estrategia de mitigación?

[Veamos 4 tipos]

FORTIFICACIÓN

* Buenas contraseñas, candados, etc.
* Fortalecer dispositivos

REDUCCIÓN

* Menos es más —estrategia de decrecimiento—
* Limpiar/ Borrar/ Destruir
* Ordenar/ Organizar
* Ignorar/Bloquear

CAMUFLAR [UN POCO DE LO CONTARIO]: MÁS ES MEJOR

* Inflación de datos —información— para devaluarla
* Mentir / Falsas pistas
* Crear ruido
* Compartimentar: mezclar y combinar

DIVERSIDAD DE PERILES [CADA UNO CON SU VALOR Y FUNCIÓN]

* Separar/ Dividir
* Disociar
* Mapear / clasificar

Prácticas seguras para mantener tu privacidad y seguridad en redes

1. Usa de contraseñas fuertes.
2. Usa contraseñas largas.
3. Elige contraseñas con mayúsculas, minúsculas, números y símbolos.
4. No uses la misma contraseñas para plataformas diferentes. [Ejemplo: No uses la misma contraseña para correo, Instagram, Twitter, Facebook, etc.]
5. Cambia tus contraseñas periódicamente. Cada 3 meses, por ejemplo.
6. No marques "recordar contraseña" en navegadores de computadoras compartidas.
7. Para guardar tus contraseñas, puedes usar gestores de contraseñas como Keepass.

¿Te gustaría probar la seguridad de tus contraseñas? Compruébala acá.

Cómo tunear tu navegador

[Puedes instalar en Firefox, Chrome y Safari]

– Lightbeam.
– Trackography.
– Panopticlick.
– Security in-a-box.

Pasos sencillos para minimizar rastreo

Instalar extensiones que mejoran tu privacidad como por ejemplo Privacy Badger —que bloquea rastreadores espías y publicitarios—, Adblock Plus —que evita ventanas emergentes desagradables— o Ghostery —que anula rastreadores de terceros actores que buscan perfilar tus hábitos en línea—, HTTPS Everywhere o Click&Clean.

Puedes también revisar las opciones de configuración de tu navegador y mejorar las que tienen que ver con privacidad y seguridad, como por ejemplo borrar con regularidad las 'cookies' [<info.securityinabox.org/es/firefox_principal> y <help.riseup.net/en/better-web-browsing>] o usar motores de búsqueda *privacy friendly* [DuckDuckGo, Ixquick e Starpage].

Navegación encriptada

Aunque consigas enmascarar la dirección de IP, las informaciones pueden ser interceptadas en el camino hasta el destino final.

HTTPS

Para que nuestras informaciones naveguen de forma cifrada es necesario usar direcciones de webs que contengan certificado de seguridad que garantice que la información entre la persona que accede y el destino final está segura.

Esos certificados son reconocidos por el protocolo HTTPS que está localizado en la barra de tu navegador. Algunos sitios web ofrecen ese servicio, otros tienen el certificado pero no lo usan como obligatorio y otros no se preocupan por ello.

HTTPS Everywhere y Tor

Para garantizar que tu navegador siempre intente acceder a las web por medio de protocolo seguro existen algunas extensiones para tu navegador como HTTPS Everywhere o el proyecto Tor y su herramienta Tor Browser Bundle con la que navegar de forma anónima por internet.

Navegación anónima

Cuando navegamos en internet básicamente transferimos paquetes de información con datos, dirección de remitente y destinatario. Llamamos a la dirección de remitente dirección IP. La dirección de IP localiza geográficamente. Si miramos los registros de IP de acceso de una página web podemos identificar de dónde vienen estos accesos.

Los proveedores de internet también pueden identificar qué cliente ha usado una dirección de IP en determinado horario —o sea, qué página web estás visitando—.

Para navegar sin revelar tu localización es necesario enmascar la IP que identifica nuestra localización. Al enmascar la IP, los paquetes de informaciones serán enviados con otra dirección de envío, es decir, que la dirección IP será identificada como tuya pero con diferente lugar de acceso.

TOR

Para simplificar: Tor permite enrutar el tráfico en la web por medio de computadoras de la red Tor para que al otro lado de la conexión no se consiga rastrear el tráfrico de vuelta a ti. De esta manera, cuantos más usuarios usan Tor, más protegida está tu información.

Como el propio nombre sugiere —Tor es el acrónimo de The Onion Router—, Tor crea capas para ocultar tu identididad —como en una cebolla, u “onion” en inglés—.

La forma más fácil de usar esta red para acceder a la web es por el navegador Tor.
Además de enchufarte automaticamente a la red Tor, este navegador toma otra serie de medidas para tornar tu navegación segura y anónima.

Navegador Tor.

Panfleto explicativo sobre el Projeto Tor.

Correos seguros

GPG

Recomendamos herramientas como GPG, usadas en conjunto con lectores de *e-mail* [Thunderbird, Mail, etc.].

Para usar la criptografía debes primeramente instalar el GPG en tu ordenador, después crear una llave pública y otra privada y cambiar la llaves públicas con la persona destinataria —que también debe hacer el mismo proceso—.

Descarga GPG Tools [Mac OS X].

Descarga GPG4USB [Windows].

Descarga GnuPG [Linux].

Servicios de 'e-mail' seguro

– Riseup.

– Aktivix.

– Autistici.

Chat seguro

Pidgin y Adium

Si quieres tener más privacidad en la comunicación vía chat, puedes usar herramientas como Pidgin y Adium con plugin OTR. Con ellos puedes acceder a tus cuentas de Gmail y Facebook, teniendo todos tus chats cifrados para conversar con tus contactos.

Hace falta que tus contactos también utilicen Pigdin o Adimum para que puedas hacer cifrado de punta a punta.

Descarga Pidgin y OTR [Windows y Linux].

Descarga Adium [Mac].

Plataformas seguras para blogs y sitios web

Blogs

Estos servicios ofrecen hospedaje para blogs con base en la plataforma Wordpress:

– Milharal.
– Network 23.
– Noblogs.

Sitios web

Autistici es un colectivo italiano formado por ativistas. Además de servidor para hospedar web, también ofrece *e-mail*, lista, *newsletter* y mensajería instantánea.

Autistici.

Apagar vestigios

Imágenes y PDF

Archivos como fotografías, vídeos, gifs, PDF y otros contiene informaciones adicionales que muestran, por ejemplo, fecha de creación, modificaciones, tipos de cámara utilizada, ISO, programa de edición, autoría y varias informaciones que pueden ser utilizadas para identificar personas. Son los "metadatos".

Para apagar los vestigios de estos archivos recomendamos los siguientes programas:

– Steel bytes [Windows].
– Image MetaData Stripper [Mac OS].
– MAT [Linux].

Archivos

Algunos archivos pueden seguir grabados en tu ordenador aunque los hayas borrado. Para eliminarlos existen herramientas como Eraser o Ccleaner.

Descarga Eraser.

Descarga Ccleaner.

Qué hacer y no hacer en las redes sociales

Facebook, Twitter, Instagran y Google guardan tus informaciones para fines lucrativos —venta de publicidad— o de investigación. Para aumentar tu privacidad y seguridad en esa plataformas, además de usar las herramientas ya dichas, puedes tomar precauciones para disminuir el riesgo de colecta de informaciones que tú consideres importantes y privadas:

– No utilizar tu perfil personal para articular acciones, crear eventos, publicar informaciones sensibles, intercambiar ideas o documentos o hacer cualquier movimento —aunque ser por mensaje privado— que pueda ser utilizado contra ti.

– No utilizar tu perfil personal para administrar páginas activistas en Facebook.

– Usar Tor siempre que acesar redes sociales para acciones activistas.

– Chequear constantemente las configuraciones de privacidad y seguridad.

– Mirar los cambios en la política de privacidad de estos servicios.

Cómo protegerse al usar el móvil

Mensajes de texto

Recomendamos TextSecure y Signal, que usan los contactos SMS del teléfono para enviar mensajes y permite conversaciones en grupo.

También la aplicación ChatSecure, que utiliza tus contactos de Facebook y Gmail para conversaciones cifradas.

Descarga TextSecure [Android].

Descarga Signal [iPhone].

Descarga ChatSecure.

Conversaciones de voz

RedPhone [Android] y Signal [iPhone]. Funcionan por VoIP —siglas de *Voice over IP*, voz sobre IP o voz sobre protocolo de internet—, ligaciones telefónias hechas por internet.

Descarga RedPhone [Android].

Descarga Signal [iPhone].

Esperamos que te haya gustado este material. Comparte. Difunde. Si te gusta lo que has leído, investiga, prueba y documenta. Así la red aumenta y el conocimiento también.

Fuentes

Además de todas las fuentes indicadas a lo largo del texto, este manual también utiliza como fuentes directas o indirectas:

– Lista de manuales seguridad/privacidad con perspectiva de género.
– Manda Nudes.
– Tem boi na linha?
– Cibermujeres.
– Take Back The Tech!
– Donestech.
– Gynepunk.
– Memes Feministas.
– Autodefensa Informática.
– Zero Trollerance.
– Fanzine "Me falta privacidad para la autonomía de mi deseo".
– Alerta Machitroll.
– Coding Rights.
– The Everyday Sexism Project.
– "Blogging Initiative Amplifies Voices of Young Arab Women".
– Chupadatos.

Manual elaborado por Larissa Saud [trayectos.org] en el marco de *Gamestar(t): arte, tecnología y videojuegos*, programa desarrollado por ArsGames en Málaga entre 2017 y 2018.