manual de *autocuidados* digitales feministas

akãhatã

equipo de trabajo en sexualidades y géneros

El autocuidado digital en colectivo es como una gran red de EMPATÍA:
al cuidarnos nosotres también estamos cuidando a les otres.

introducción

Este manual de autocuidado digital y feminista es una propuesta centrada en acciones colectivas. Reconocemos que la seguridad digital depende de la apertura de cada une al cuidado de les otres. Por tanto, los métodos para protegernos tienen que ser pensados desde la empatía. Pensar en colectivo da fuerza a cada acción que generamos desde nuestras propias individualidades e identidades.

Este manual es feminista porque asume que existen las desigualdades de género y reconoce su violencia como algo estructural; al igual que el racismo, el capacitismo y otras opresiones, que también se reproducen en lo digital.

Ante la imposibilidad del lenguaje normativo de abarcar todas las identidades que exceden el binarismo sexual, optamos por el lenguaje inclusivo para interferir la norma. Usamos la “e” porque reconocemos la multiplicidad de identidades borradas con el uso del masculino universal o no incluidas en el binario.

» ¿De qué va el manual?

Este manual es un acercamiento básico e introductorio a diferentes prácticas de cuidado digital desde una perspectiva feminista. Cuenta con reflexiones sobre cómo llevar a cabo acciones que permitan cuidarnos mutuamente e incluye herramientas para acompañar estas prácticas.

» Conceptos y definiciones clave

_Riesgo
Posibilidad de daño que puede afectarme a mí o a mi colectiva. Esta posibilidad depende del nivel de vulnerabilidad en el que me encuentre. La fórmula básica del riesgo es:

$$\text{Riesgo} = \frac{\text{Amenaza} \times \text{Vulnerabilidad}}{\text{Capacidad de respuesta}}$$

_Amenaza
Cualquier fenómeno, persona o proceso que constituya un riesgo.

_Vulnerabilidad
Es la capacidad (alta o baja) que tenemos para enfrentarnos a los riesgos o eventos que puedan ocurrir.

_Privacidad
Es el ámbito de la vida personal de un individue, quien se desarrolla en un espacio reservado. La privacidad es un derecho humano.

_Datos personales
Es toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables.

_Derechos digitales
Son aquellos derechos que permiten a las personas acceder, usar, crear y publicar medios digitales; así como acceder y utilizar ordenadores, otros dispositivos electrónicos y redes de comunicaciones[1].

1 | Derechos digitales, imprescindibles en la era de Internet

_Metadatos
Se refieren a los datos y características que constituyen nuestros datos. Por ejemplo, los metadatos de una fotografía son la ubicación en donde fue tomada, el tipo de celular que se utilizó para tomarla, etc.

_Hackeo
Uso de tecnologías para descifrar información privada con el fin de dañar a una persona u organización. Un posible hackeo de información puede ser hacia las cuentas de redes sociales de tu colectiva: publicar o borrar tu historial de publicaciones. En este ejemplo, el riesgo directo es perder la memoria de todo el trabajo alcanzado.

_Encriptación
Es el proceso de codificar algún dato, documento o archivo para que el contenido sea indescifrable y sólo pueda accederse al mismo mediante una clave.

contexto, riesgos y amenazas

Analizar la tecnología como proceso es una forma de entender que cada tecnología que aparece en nuestras vidas responde a intereses que se encuentran situados en contextos específicos. Por ejemplo, las grandes potencias que buscan desarrollar mecanismos para aumentar la vigilancia de la población; periodos concretos, como en las pandemias, cuando aumenta el rastreo de personas o el uso indiscriminado de nuestros datos personales.

Dentro de nuestros activismos es importante leer estas tecnologías críticamente y ser creatives para encontrar formas de usarlas a nuestro favor. Aquello que se presenta como una amenaza para nuestras identidades y trabajo puede ser reutilizado de forma adaptada, colaborativa y participativa. Las reapropiaciones estratégicas de distintas tecnologías pueden, potencialmente, incrementar nuestras capacidades y el alcance de nuestras voces.

» Análisis de riesgos y amenazas

¿Cuáles son los riesgos y las amenazas que podemos encontrar dentro de nuestros activismos?

Ningún trabajo activista se encuentra libre de posibles riesgos. Sin embargo, es importante saber reconocerlos para mitigarlos. Los riesgos pueden ser externos a nuestras colectivas, por ejemplo, a través de la vigilancia de los gobiernos; o internos, por ejemplo, a través de infiltraciones de personas. Ciertos riesgos pueden ser considerados leves, como el hackeo de una cuenta o perfil digital, e incrementar su peligrosidad si la información o datos con los que trabajamos es sensible o contiene datos personales.

Estos riesgos pueden resultar en:

_ Pérdida de nuestros datos personales y los datos de nuestras colectivas o compañeres.

_ Cese de las acciones planificadas a llevarse a cabo por nuestras colectivas.

_ Amenazas a la integridad física de las personas y dispositivos.

» Posibles fuentes de ataque hacia nosotres

¿Quiénes podrían ser nuestros potenciales adversarios? Nuestros adversarios, creeríamos, son esas grandes entidades y seres que están por sobre nuestras cabezas: las instituciones públicas y gobiernos, las organizaciones religiosas, grupos fascistas y anti-derechos. Sin embargo, es necesario pensar que nuestros adversarios pueden ser las personas más cercanas a nosotres. Nuestras parejas, familiares e incluso nuestres amigues.

La vigilancia, el acoso y la persecución no se dan de forma vertical desde una institución hacia nuestras identidades digitales y nuestras cuerpas físicas; sino que también pueden encontrarse dentro de esas relaciones que consideraríamos horizontales y pares. Una pareja o compañere puede ejercer violencia y vigilancia al solicitar tus contraseñas o al pedirte pruebas sobre tu ubicación.

¿por qué autocuidados feministas?

» ¿Qué son los autocuidados colectivos feministas?

Los autocuidados digitales son las formas en las que trasladamos todos los cuidados físicos, emocionales y psicológicos a la dimensión digital. Esto implica repensar cuáles son estas prácticas, cómo las llevamos a cabo y quiénes conforman nuestras redes de cuidado.

El autocuidado es feminista si es pensado desde una perspectiva colectiva, emancipadora y transformadora de los roles y opresiones de género tradicionales. La versión feminista del autocuidado también requiere reconocer que la vivencia de las opresiones y de la violencia se agrava al intersectar con otros vectores como capacidad, raza, sexualidad, etc. Pensar en el autocuidado colectivo digital significa protegernos de manera empática, cuidarnos entre compañeres y de esta forma cuidarnos a nosotres mismes.

Las dimensiones del autocuidado colectivo digital se encuentran ligadas de forma paralela a nuestros cuidados físicos. Tomar mayor control de los dispositivos con los que conectamos nuestra realidad al mundo digital nos permite, no sólo protegernos, sino también proteger a les otres. Las acciones que realizamos en el mundo físico, como transportar nuestros dispositivos móviles o tomar fotografías, pueden ser acciones que aumenten la vulnerabilidad de la privacidad de nuestras identidades digitales y las de otras personas.

Por ejemplo:

_ No dejar abiertas o desbloqueadas nuestras computadoras o dispositivos móviles en lugares públicos
→ Permite que otras personas no puedan acceder fácilmente a nuestras cuentas o perfiles.

_ Que nuestras computadoras o dispositivos móviles tengan una contraseña segura
→ Permite que, en caso de robo, nuestras cuentas y sesiones estén protegidas.

Mapa de organizaciones en apoyo a los cuidados digitales de la región

_México
. SocialTic
. Codeado México
. Luchadoras
. Rancho Electrónico
. Colectivo Disonancia
. Colectivo Mecha
. SeguDigital

_Guatemala
. CiberfeministasGT

_El Salvador
. Las Mélidas

_Nicaragua
. La quimera feminista
. Enredadas por el arte y la tecnología

_Panamá
. Ipandetec

_Brasil
. Cl4ndestina

_Colombia
. Fondo de acción urgente latinoamericano
. Fundación Karisma

_Ecuador
. Taller comunicación mujer

_Perú
. Hiperderecho

_Paraguay
. TEDIC

_Chile
. Proyecto Aurora de Amaranta

_Argentina
. Activismo feminista digital
. Las de Sistemas

_Regionales

. Derechos digitales
. Ciberseguras
. Tactical Tech
. Escuelafeminista.red
. Progresiva
. Dominemos las TIC
. Asociación para la Comunicación
. Access Now

guía de herramientas

» Herramientas

Contraseñas seguras

Cuidar las contraseñas es uno de los pasos fundamentales para un buen cuidado de nuestras identidades digitales. Para lograrlo existen pasos muy simples a seguir:

_ No utilices la misma contraseña para más de una cuenta.

_ Aprende sobre gestores de contraseñas como KeepassXC para manejar todas las contraseñas que vayas a crear.
» El gestor de contraseñas es una caja fuerte donde puedes guardar todas tus contraseñas bajo una misma clave maestra. Si no estás creative, también te ayuda a crear contraseñas seguras para utilizar con tus cuentas.

_ Utiliza contraseñas que tengan caracteres especiales como puntos, comas, signos de admiración, interrogación e incluso espacios.

_ Nunca dejes tus contraseñas libres. ¡Qué lo que sea libre sea el amor!

Autoevaluación sobre contraseñas seguras:

◊ ¿Tengo una contraseña alfanumérica en mis dispositivos?

◊ ¿Actualizo periódicamente las contraseñas?

◊ ¿Tengo contraseñas diferentes para mis cuentas y las cuentas de mi organización?

Navegación segura

Existen muchas formas de navegar el vasto mar del Internet de forma segura y con un bajo nivel de exposición a ataques o riesgos. Primero, es importante comprender la diferencia entre una navegación segura y una navegación incógnita.

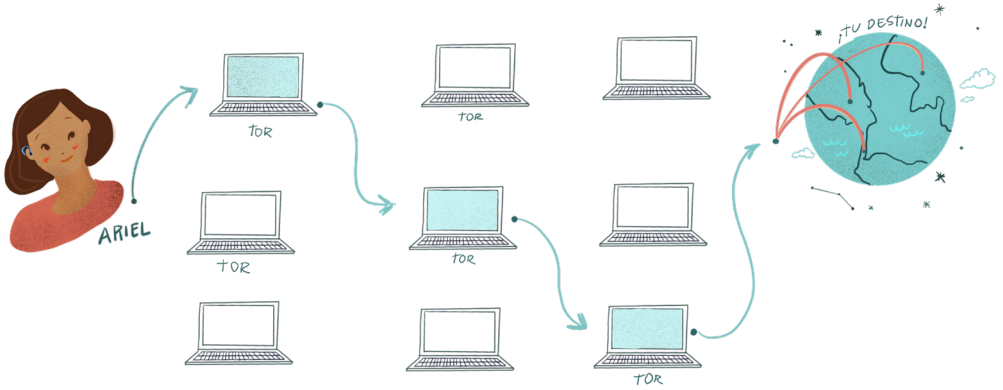
Navegar de forma segura implica tomar consideraciones prácticas como no acceder a páginas de dudosa procedencia o que parezcan sospechosas, Para ello, *puedes revisar que en la barra en donde escribes la dirección web, después del http, haya una "s"*. Esto significa que el sitio web tiene un certificado de seguridad (Secure Sockets Layer). Puedes revisar que la dirección donde navegas, o URL, sea real. Por ejemplo: https://www.nytimes.com/ y no una dirección dudosa como http://www.newyorktimes.info. Siempre revisa la veracidad de los links antes de entrar e ingresar cualquier tipo de datos personales.

Existen herramientas como VPN y navegadores como TOR que aportan una capa extra de seguridad y anonimato al momento de navegar. Aquí un ejemplo de cómo funcionan:

_**VPN:** una VPN, o red privada virtual, conecta tu dispositivo a un servidor remoto en el país de tu elección a través de un túnel seguro. Lo anterior enmascara tu dirección IP haciendo que parezca que accedes a Internet desde un servidor remoto y no desde tu ubicación real.

- **Bitmask:** https://bitmask.net/es
- **RiseUp VPN:** https://riseup.net/es/vpn

_TOR: The Onion Router (Tor) es un software gratuito que oculta tu identidad al cifrar tu tráfico y dirigirlo a través de varios servidores operados por usuarios conocidos como nodos.



¿Cuál es mejor? Los dos cumplen funciones distintas. Por ejemplo: las VPNs ofrecen cifrado de extremo a extremo y hacen que tus datos sean 100% invisibles a hackers y espías.

A menos que uses el sistema operativo Tor, este sólo protegerá los datos que se transmiten a través de tu navegador. Las VPNs, en cambio, cifran todos los datos que viajan a través de tu conexión[2].

2 | Definiciones de VPN y TOR

También puedes anonimizar tu navegación a través del uso de *pestañas de incógnito* (Chrome) o *pestañas privadas* (Firefox). Este tipo de navegación se aconseja cuando no utilizas tus dispositivos o estás en una computadora de acceso público. Al navegar a través de este tipo de pestañas no se guardarán tus datos. Esto no quiere decir que las páginas que visites no reconozcan que accediste a ellas, sino que el dispositivo físico no guardará tu información.

Recomendación en combo: utilizar Firefox ya que es un navegador web libre y de código abierto. Además, utiliza menos memoria que Chrome por lo que lo hace un navegador más rápido. Utiliza DuckDuckGo[3] como motor de búsqueda ya que no recolecta datos personales al hacer búsquedas. Por lo tanto, no crea un perfil de tus preferencias, sino que te muestra la información relevante de tu búsqueda.

3 | DuckDuckGo

Autoevaluación sobre navegación segura:

◊ ¿Cierro las sesiones de mis cuentas cuando las utilizo en dispositivos que no son míos?

◊ ¿Utilizo sesiones incógnitas o secretas cuando navego en dispositivos que no son míos?

◊ ¿Utilizo buscadores seguros para no dejar rastros de mis preferencias en los navegadores?

Comunicación y mensajería segura

Mensajear de forma segura tiene dos componentes: uno técnico y otro de comportamiento de usuarie. Por ejemplo, existen diferentes tácticas que podemos adoptar para poder comunicarnos de forma más segura a pesar de no contar con una aplicación segura.

La aplicación más recomendada es Signal porque cuenta con cifrado de extremo a extremo en todas tus conversaciones, incluidos tus chats grupales. Esto significa que nadie podrá interceptar tu comunicación, tampoco la empresa. Signal también ofrece bloqueo de acceso a la aplicación con una contraseña.

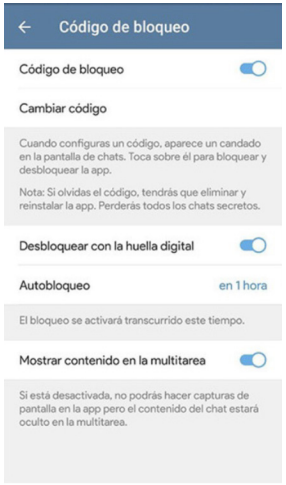
Si cuentas con poco acceso a Internet, baja capacidad de almacenamiento en tu dispositivo y tu única alternativa es Whatsapp, u otra plataforma de alto riesgo, es importante saber utilizarla de forma segura. Para ello tenemos las siguientes recomendaciones:

_ **Que tu foto de perfil no aparezca en un entorno íntimo,** con personas cercanas, familia ni menores de edad. Evita dejar un rastro con el que puedan reconocerte.

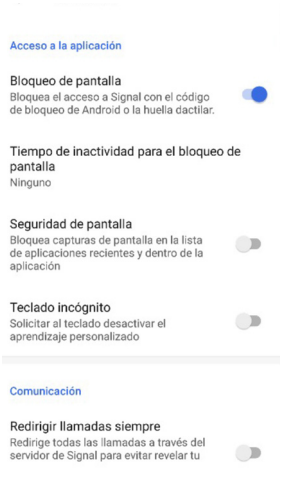
_ **Procura que tu nombre en la plataforma no sea tu nombre real.** Utiliza pseudónimos creativos.

_ **Utiliza una contraseña de acceso a la plataforma.** Por ejemplo, en los ajustes de Whatsapp puedes establecer una contraseña y un pin de acceso para ingresar a la aplicación.

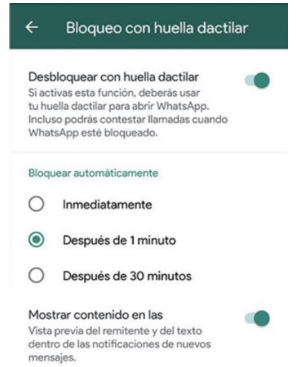
Telegram

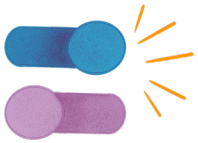


Signal



Whatsapp





Si necesitas compartir algún tipo de contraseña o información sensible puedes proponer un esquema seguro para hacerlo. Por ejemplo, enviar primero los tres últimos dígitos de una contraseña, luego los tres primeros y de último los tres de en medio.

La siguiente tabla también te puede ayudar a entender mejor cómo funcionan las tres aplicaciones de mensajería más populares[4].

	Whatsapp	Telegram	Signal
Confirmación de envío	✓	✓	✓
Confirmación de lectura	✓	✓	✓
Indicador de tecleo	✓	✓	✓
Llamadas de voz	✓	✓	✓
Videollamadas	✓	✓	✓
Chats grupales	✓	✓	✓
Enviar fotos y videos	✓	✓	✓
Notas de voz	✓	✓	✓
Notas de video	✗	✓	✗
Envío de GIFS	✓	✓	✓
Envío de ubicación	✓	✓	✓
Envío de contactos	✓	✓	✓
Envío de archivos	✓	✓	✓
Nube personal	✗	✓	✗
Vídeo grupal	✓	✗	✓
Sistema de stickers	✓	✓ *y animados	✗
Acceso obligatorio a contactos	✓	✗	✗
Bloqueo de capturas de pantalla	✗	✓	✓
Cifrado de extremo a extremo	✓	Sólo en chats secretos	✓
Mensajes temporales	✓	Sólo en chats secretos	✓
Notificación sin mensajes	✗	✗	✓
Bloqueo de app en el móvil	✓ nativo	✓	✓
Remitente confidencial	✗	✗	✓
Bloqueo de registro	✗	✗	✓

Para reportar abusos en plataformas de mensajería[5]

WhatsApp: sigue estos pasos para reportar un grupo de chat o a un contacto: https://faq.whatsapp.com/21197244/#Report

Telegram: puedes reportar un contacto, grupo o canal desde las opciones del celular. Para stickers o bots envía un correo a abuse@telegram.org. Incluye el enlace y el @username a reportar.

Signal: puedes bloquear un número de teléfono, contacto o grupo.

4 | Signal vs Telegram vs WhatsApp

5 | Para reportar en chats

Para realizar videollamadas o videoconferencias seguras se puede utilizar *Jitsi* (https://meet.jit.si/). Esta plataforma es de software libre, no requiere la creación de un usuarie, ni la instalación de una aplicación en la computadora, sólo en el dispositivo móvil. Se puede agregar contraseña, desdibujar el fondo, compartir pantallas, transmitir, etc.

Una opción para el uso de correos electrónicos seguros es la encriptación de los mensajes y el uso de llaves de cifrado. Sin embargo, una versión rápida y eficaz es Mailvelope (https://www.mailvelope.com/). Este software ya cuenta con código abierto y cifra de extremo a extremo el tráfico de correo electrónico dentro de un navegador web. Además, se puede integrar a las aplicaciones de correo existentes como Outlook o Gmail.

Autoevaluación sobre mensajería segura:

◊ ¿Utilizo aplicaciones seguras con encriptación de punta a punta?

◊ ¿No envío contraseñas ni contenido sensible a través de aplicaciones de mensajería de alto riesgo?

◊ ¿Utilizo nombres clave para los usuarios de mis aplicaciones de mensajería?

◊ ¿Reviso que durante mis videollamadas no aparezca información de otras personas como fotografías en el fondo?

Compartir contenido y documentos de forma segura y colaborativa

Al compartir contenido pueden ocurrir filtraciones de información: datos de las personas que envían el contenido y también de quienes lo reciben. Uno de los primeros pasos antes de enviar documentación o contenido es borrar metadatos. De este modo, los documentos, en caso de ser interceptados, no contarán con información que permita identificar lugares, personas o dispositivos. Para reducir el riesgo al compartir fotografías, se puede utilizar la aplicación SendReduced disponible para Android. Para iPhone estos son los pasos a seguir: inicia la aplicación, selecciona tus fotos, toca el ícono de ajustes en la esquina inferior izquierda y selecciona borrar todos los metadatos.

Para enviar documentos de forma segura y con mayor privacidad (y también autodestrucción) puedes utilizar los servicios de Rise Up:

- **pad.riseup.net** – editor de texto colaborativo en tiempo real con autodestrucción programada
- **share.riseup.net** – carga de archivos (pastebin e imagebin)

Sobre sexting: si queremos practicar sexting seguro o intercambio de mensajes con contenido erótico, te recomendamos que utilices stickers para tapar tu rostro o cualquier marca de tu cuerpo con la que puedan identificarte. Asimismo, recomendamos utilizar plataformas de mensajería que permitan autodestruir los mensajes (como Telegram, o Signal) y donde las personas que reciben tu contenido no puedan realizar capturas de pantalla ni compartirlo.

* **Recuerda:** si tu información es compartida sin tu consentimiento ¡no es tu culpa! Existen organizaciones que pueden ayudarte a remover el contenido de plataformas en donde tus archivos fueron filtrados. Una de estas redes de apoyo es la línea de ayuda de la organización de derechos digitales Access Now o Acoso.Online.

Autoevaluación sobre compartir contenido de forma segura:

◊ ¿Comparto contenido y documentos a través de plataformas seguras?

◊ ¿Descargo documentos de procedencias dudosas o de personas que no conozco?

◊ ¿Descargo aplicaciones sólo de sitios seguros como Apple Store o Google Play?

◊ ¿Utilizo algún borrador de metadatos?

Uso de redes sociales de forma segura

De Facebook a TikTok, pasando por Instagram, Twitter o Pinterest, las redes sociales están diseñadas para brindarnos espacios de "encuentro" entre las personas que nos interesan, las cosas, actividades y aquello que más nos apasiona. Sin embargo, es necesario saber que estas redes se alimentan de nuestros patrones de comportamiento y aprenden de ellos. ¿Qué quiere decir eso? Que si le damos *me gusta* a muchos vídeos de perritos, es muy probable que lo único que las redes nos muestren sean perritos o vídeos afines a perritos. ¿Qué tiene esto de malo? Los perritos no tienen nada de malo. Sin embargo, al pasar al ámbito político o al de nuestro activismo, las redes sociales pueden convertirse en cajas de resonancia de nuestros propios intereses y así sesgar nuestras experiencias. Tampoco existe una fórmula clave para contrarrestar al 100% estos algoritmos y las formas en las que aprenden de nuestros patrones de conducta, pero sí existe la posibilidad de una mayor consciencia de nuestra experiencia utilizando redes.

Desde el ámbito del cuidado colectivo digital, es importante recordar que las redes sociales son empresas privadas que buscan beneficiarse y cuidar sus intereses. Es así que puedes constatar que actualizan sus términos y condiciones de uso de forma constante. Una regla general es siempre leer cuidadosamente antes de darle un "ok" o un "acepto". En muchas ocasiones, las plataformas actualizan condiciones de privacidad que afectan la seguridad de nuestros perfiles. Por ello, la revisión periódica de estas condiciones es de vital importancia para el autocuidado en redes.

Algunas consideraciones para los usos de las redes sociales más populares

	FB	IG	TW	TK
Creación de pseudónimo como usuarie	✗	✓	✓	✓
Cambiar en cualquier momento tu usuarie	✗	✓	✓	✓
Agregar tu pronombre personal o género	✓	✓	✓	✓
Agregar factor de doble autenticación para inicio de sesión	✓	✓	✓	✓
Crear un perfil privado	✓	✓	✓	✓
Configuraciones de seguridad para las publicaciones (quién puede ver tu publicación, quién puede responder)	✓	✓	✓	✓
Mensajería efímera (auto borrado de mensajes después de un tiempo determinado)	✗	✓	✗	✗
Configuración de seguridad para recepción de mensajes (sólo recibir mensajes de personas que sigues, o de personas que te siguen)	✓	✓	✓	✓
Configurar ubicación de tus publicaciones	✓	✓	✓	✓
Revisión de las publicaciones en las que te etiquetan antes de publicarse en tu perfil	✓	✓	✗	✗

FB: Facebook **IG:** Instagram **TW:** Twitter **TK:** TikTok

Autoevaluación de usos de redes sociales de forma segura:

◊ ¿Reviso las diferentes configuraciones de seguridad para las redes sociales donde tengo un usuarie o mi organización tiene un perfil?

◊ ¿Conozco los mecanismos para denunciar ataques a través de las redes sociales?

◊ ¿Cuento con protocolos de seguridad y actualización de configuraciones de privacidad de mis redes y las redes de mi colectiva?

◊ ¿Utilizo la misma contraseña de acceso en más de una de mis redes?

◊ ¿Subo fotos y contenido sin pautas de privacidad que podrían exponer a otres compañeres?

Desintoxicación digital

"Desintoxicación digital" es el nombre que le damos a aquellas prácticas personales o colectivas que aportan a desconectarnos de nuestras identidades y cuerpas digitales para salvaguardar nuestra salud mental, emocional o física.

Desintoxicarnos digitalmente puede ser tan sencillo como quitar el sonido de las notificaciones a nuestros dispositivos móviles, no revisar nuestros correos durante los fines de semana e incluso configurar la pantalla de nuestros teléfonos a blanco y negro para reducir los estímulos de uso.

Muchas aplicaciones, desde su creación y diseño, utilizan patrones que hacen que nos "enganchemos"[6] para que la tecnología sea más persuasiva en sus dinámicas de uso. Por ello, es importante reconocer cuáles son los usos que le damos a nuestras aplicaciones. Las tecnologías no son neutras, sino que han sido diseñadas para captar nuestra atención.

6 | Tecnología persuasiva

Autoevaluación

◊ ¿Reconozco los riesgos digitales que pueden afectarme a mí y a mi organización o colectiva?

◊ ¿Reviso los pasos y prácticas de autocuidado digital colectivo cuando pienso en la planificación de las actividades de mi organización o colectiva?

◊ ¿Busco momentos durante el día para desconectarme del mundo digital y enraizarme a mi presente tangible?

◊ ¿Adopto tecnologías de forma consciente con respecto a los riesgos que puede traerle a mi organización, a mi misme y a mis compañeres?

Mantra del autocuidado digital para repetirnos todos los días:

»Lo digital es real«.

El autocuidado feminista es colectivo, político, transformador y empoderador.

conclusiones

Con este manual nos propusimos repensar la noción de seguridad digital hasta transformarla en una herramienta feminista de autocuidado. Reconocer que lo digital es real es reconocer que el acoso, el abuso y las violencias que se reproducen en el espacio cibernético también son reales. La violencia digital no está por fuera de las lógicas (cis)sexistas, racistas, clasistas, capacitistas y heterocentradas que permean el mundo de lo tangible. De ahí nuestra insistencia en movilizar las estrategias que hemos construido desde los feminismos para resguardar nuestras cuerpas, nuestras colectividades y nuestros activismos en la red. El auto-cuidado feminista, como mecanismo de autodefensa digital, es una manera de armarnos contra las violencias sistemáticas que nos colocan en posiciones de riesgo en Internet.

Mantenernos a salvo es una política feminista de cuidado colectivo y es en la colectividad desde donde nos situamos para generar estrategias de autocuidado en el ciberespacio. Si el autocuidado feminista implica una serie histórica de reapropiaciones políticas, el uso que hacemos de las herramientas digitales es también una reapropiación subversiva. Podemos usar y transformar las plataformas virtuales aun cuando estas operan como espacios de reproducción de violencias contra corporalidades históricamente vulneradas. Al tiempo que la tecnología reproduce los lugares comunes de la violencia, nosotres reconfiguramos esos marcos normativos para ampliar nuestros espacios de agenciamiento.

Cada vez hay más activistas y colectivas que hacen uso de diversas tecnologías para organizarse, difundir información, hacer denuncias y exigir derechos. Cada vez son más los movimientos sociales que toman el ciberespacio de formas disruptivas para movilizar estrategias de cambio. Sin embargo, el Internet no está libre de riesgos y la vida de les activistas no está fuera de peligro.

Es por ello que buscamos generar redes para democratizar el uso de las tecnologías al tiempo que reducimos la posibilidad de daño para quienes hemos tomado el mundo digital en aras de la transformación social. Este manual es en sí mismo una práctica de autocuidado digital feminista porque entendemos que el cuidado de sí no es posible sin el cuidado de les otres.

A medida que los ataques hostiles de grupos fascistas y anti derechos se desplazan hacia plataformas virtuales, también emergen nuevas formas para difundir discursos de odio, amenazas y otras formas de violencia digital. De ahí la importancia de imaginar herramientas que ayuden a mitigar los efectos de la vulnerabilidad cibernética. Reducir riesgos en el uso del Internet equivale a amplificar los alcances de las acciones que les activistas realizamos en la red. En ese sentido, el autocuidado digital feminista que proponemos es también un modo de conectar el mundo virtual con las transformaciones del mundo *offline*.

Para finalizar, enlistamos algunos puntos esenciales para el fortalecimiento del autocuidado digital feminista:

_ Reconocer de dónde vienen las tecnologías que utilizamos y cuáles son los medios que tenemos a nuestro alcance para transformar sus usos. Adaptar el uso de herramientas digitales a nuestro favor ¡es posible!

_ Las aplicaciones y plataformas que utilizamos se encuentran en constante actualización. Por ello, es necesario revisar periódicamente qué cambios pueden afectar mi seguridad y privacidad y la de mi colectiva. Realiza chequeos periódicos de tus prácticas. Puedes utilizar: https://protege.la/checklists/

_ Pensar en el otre de forma empática y cómo puede verse afectado por el uso que le demos a algún tipo de tecnología o medio digital.

_ Ninguna práctica de cuidado digital es infalible. Es necesario realizar un compendio de prácticas que juntas sirven como un escudo para cuidarnos y cuidar de les demás.

_ No tengamos miedo a experimentar nuevas herramientas, pero seamos conscientes de cuáles son sus limitaciones y sus riesgos. Contactemos a compañeres que conozcan sobre estas tecnologías y tengamos siempre una segunda opinión.

reconocimiento

Este manual es un compendio de aprendizajes de experiencias personales, colectivas y también de una recopilación de conocimiento y expertise de muchísimas organizaciones de defensa de derechos digitales de América Latina.
[Ver mapa para conocer más sobre ellas].

Gracias a todas las personas involucradas para desarrollar este material.

» *Ilustraciones:*
Lu Sánchez – Costa Rica

» *Diagramación:*
Cristiana Castellón – Nicaragua

» *Contenido:*
Selene Yang – Nicaragua

» *Supervisión del proyecto:*
Rosa Posa Guinea – Paraguay

» *Edición:*
Lucía Fernanda Bonilla – Guatemala

Con el apoyo de

FOUNDATION FOR A JUST SOCIETY

manual de autocuidados digitales feministas