

Tejiendo
Redes



GUÍA DE ALFABETIZACIÓN DIGITAL





Tejiendo



Redes

Este documento ha sido posible gracias al generoso apoyo de ProDerechos a través del CDM, COIPRODEN y ASONOG bajo el programa Tejiendo Redes para el aprovechamiento y el uso seguro e informado de las nuevas TICs en la labor de promoción, defensa y protección de Derechos Humanos de las mujeres lideresas o activistas comunitarias en el espacio digital.

Redacción Técnica: Equipo Barracón Digital

Elena Freedman
Itzel Cabrera
Nikole Yáñez

Coordinadora Nacional del proyecto Tejiendo Redes

Keillyn Nicolle Mejía

Ilustración y Diagramación

Elena Romero

ÍNDICE

1.	Introducción	5
2.	Preguntas que deberíamos hacernos antes de explorar el mundo digital	6
3.	Relaciones de poder y tecnología	6
4.	Telegram	9
5.	Cuidados digitales	11
6.	Herramientas libres y seguras	17
7.	Firefox	20
8.	Podcast sobre tecnologías	23
9.	Denuncia Digital	24
10.	Búsqueda de información pendiente	25
10.1	Directorios de organizaciones	28
10.2	Base de datos	30
10.3	Bibliografía Digital	32

INTRODUCCIÓN

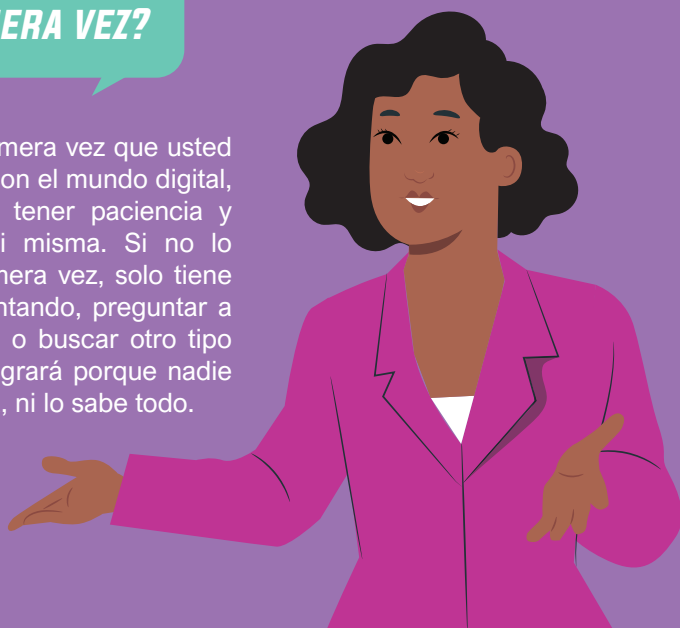


Compañeras, bienvenidas al curso de alfabetización digital del Centro de Derechos de Mujeres CDM. Les felicitamos por tomar este paso de ponerse al día con el uso de la tecnología digital, ya que este no es solo un recurso personal, sino un recurso que podamos usar en nuestro trabajo organizativo y de defensa de los derechos de las mujeres.

En este curso, aprenderemos a hacer un uso seguro de nuestros teléfonos, computadoras y/o tablets, tener los cuidados digitales que nos garantizan cierto nivel de protección y cómo buscar información en línea. Reflexionaremos sobre las relaciones de poder en que estamos inmersos y en qué están inmersas las tecnologías digitales y aprenderemos unos consejos para realizar denuncias en las redes sociales sobre violaciones de los derechos de las mujeres.

¿PRIMERA VEZ?

Si esta es la primera vez que usted tiene contacto con el mundo digital, le animamos a tener paciencia y confianza en si misma. Si no lo entiende la primera vez, solo tiene que seguir intentando, preguntar a una compañera o buscar otro tipo de apoyo. Lo logrará porque nadie nació aprendida, ni lo sabe todo.



Le invitamos a tener curiosidad frente a las cosas nuevas para sacar los beneficios del mundo digital y abrir puertas y ventanas para seguir construyendo nuestra liberación de distintas formas.

¡ COMENZAMOS!

2. PREGUNTAS QUE DEBERÍAMOS HACERNOS ANTES DE EXPLORAR EL MUNDO DIGITAL.

- 1. ¿Qué es la tecnología y para qué nos sirve?*
- 2. ¿Para qué nos sirve la tecnología digital?*
- 3. ¿Qué cosas nos preocupan y/o nos dan miedo sobre la tecnología digital?*

3 RELACIONES DE PODER Y TECNOLOGÍA

Ninguno de estos dos extremos es verdad. La tecnología no es una fuerza autónoma, sino que es creada y aplicada por los seres humanos. Por lo tanto, puede reforzar las relaciones de dominación en el mundo, o puede contribuir a nuestra liberación.

La sociedad capitalista y patriarcal en que nosotras vivimos está basada en la dominación de unos sobre otros. Los más ricos en el planeta hacen su riqueza a costo del trabajo de las personas pobres y los hombres perpetúan su poder sobre las mujeres gracias a las creencias y mitos sociales que hacen creer que ellos son más, merecen más y pueden más.

La tecnología digital es producto de esta sociedad y como tal, está inmersa en estas relaciones. Esto es obvio cuando nos preguntamos, ¿quiénes tienen acceso a la tecnología? ¿qué necesidades y de quienes se satisfacen mediante la tecnología? ¿quiénes se enriquecen de la tecnología digital?



¿ SABÍAS QUE?

- De cada 100 personas en el mundo, 63 utilizan internet y 37 no lo usan. Mas que 9 de cada 10 que no lo usan viven en países pobres de Africa, Asia y América Latina.
- De cada 100 personas que utilizan internet en el mundo, 76 viven en las ciudades y 39 viven en el campo.
- De cada 100 personas que utilizan internet en el mundo, 62 son hombres y 57 son mujeres.

Conoce más aquí:

<https://www.itu.int/itu-d/reports/statistics/facts-figures-2021/index/>

Reflexiona:

¿Por qué creen que es así?

Los ricos más ricos del mundo son dueños de importantes tajadas del mundo digital:

- Elon Musk tiene una fortuna de 219 mil millones de dólares. Entre otros negocios, “Paypal” es suyo. Es un tipo de tarjeta de débito virtual donde puedes guardar tu dinero y hacer pagos. También es dueño parcial de “Twitter”, una famosa red social, hoy en día.
- Jeff Bezos tiene una fortuna de 171 mil millones de dólares. Es un gran empresario, dueño de “Amazón”, un website para hacer compras en línea.
- Bill Gates tiene una fortuna de 129 mil millones de dólares. Es dueño de Microsoft.
- Siguen Larry Page con 111 mil millones de dólares y Serguéi Brin con 107 mil millones de dólares. Juntos son los primeros dueños de Google, el navegador más grande.

Recuerda:

¡Cuando usamos los sistemas; programas, aplicaciones y servicios en línea, estamos haciendo más ricos a los dueños del mundo digital !

Conoce más aquí:

https://as.com/diarioas/2022/04/06/actualidad/1649240532_037348.html

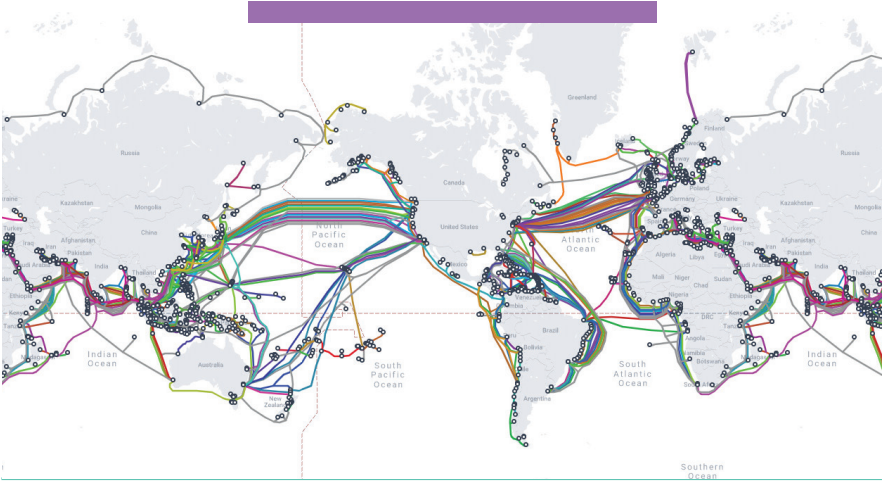
BIG DATA

Esto se refiere a la organización de información que incluye tantos datos que no puede ser procesado por aplicaciones digitales “normales”. Necesita un sistema especializado. En el Bigdata, quienes procesan data, u organizan la información para producir nueva información y darle un sentido lógico, tienen poder.

¿A QUIÉNES Y PARA QUÉ SIRVE EL BIG DATA?

- 1** A las empresas les sirve para desarrollar estrategias de “marketing” que fomentan el consumismo. Consigan tremenda información personal sobre grandes grupos de “potenciales compradores” monitoreando las páginas que abrimos, las personas con quienes comunicamos y las acciones que realizamos por teléfono o computadora. Así logran desarrollar mensajes dirigidos a cada grupo de personas, tomando en cuenta sus estilos de vida, sus gustos y disgustos, sus situaciones de salud, etc. Identifican la forma más convincente para hacerles comprar. También recogen muchísima información sobre sus competidores y pueden evitar posibles pérdidas o que otro le gane el mandado. Facilita también la especulación financiera.
- 2** A muchos gobiernos les sirve para manipular la población, utilizando las mismas estrategias como las empresas para desarrollar mensajes que crean aprobación de sus políticas o desaprobación de sus “enemigos” entre distintas poblaciones. Saben qué mensaje “vende bien” con “qué grupo de gente” porque han recabado tanta información personal sobre todas y todos. También les sirve para saber qué hacemos, dónde lo hacemos y con quienes lo hacemos. Es parte de un sistema de vigilancia que les permite acumular una gran cantidad de información sobre las y los ciudadanos para el control social. Es una forma de espionaje que poco aporta para identificar criminales pero mucho aporte para identificar comportamientos de sectores sociales.

**LA BRECHA ENTRE ESPIONAJE E INVASIÓN
DE LA PRIVACIDAD QUEDA CADA VEZ MAS CORTA**



Colonización y virtualidad

En relación a los cables submarinos, (que también representan la colonización Española) como la macro infraestructura que permite a Honduras tener acceso a Internet como país, en la actualidad es Hondutel la co-propietaria del cable submarino ARCOS y propietario del cable submarino MAYA.

Otro punto importante con respecto a que todos los cables interoceánicos de latinoamerica van a dar a Estados Unidos específicamente en Miami entonces el gobierno de Estados Unidos pinchó los cables para interceptar la comunicación que va por esos cables entonces por eso es el gran escándalo y que gracias a Wikileaks nos dimos cuenta que Estados Unidos estaba haciendo esta práctica y que es ilegal.



El uso de Telegram es muy común entre quienes viven bajo gobiernos represivos y vigilancia masiva, activistas, defensorxs de derechos humanos, etc.

INSTALACIÓN Y USO



Está disponible en GooglePlay para Android y en la AppStore para iOS. Una vez instalada en nuestros celulares podemos sincronizarla con nuestra computadora. La versión de escritorio está disponible para GNU/Linux y se puede descargar desde nuestro gestor de software principal o desde la terminal. Si usamos Windows o MacOS podemos descargarla de su página oficial.

Descargar aquí:

<https://telegram.org/es/download>

Desde las versiones del escritorio y del celular podemos intercambiar mensajes de texto con una sola persona y con un grupo de personas. También podemos hacer llamadas de voz y video desde la aplicación del celular, pero solamente con una persona.

Seguridad

Telegram usa cifrado de extremo a extremo, lo que impide que terceros

(empresas de telecomunicaciones, proveedores de internet o desarrolladores de telegram) puedan ver nuestros mensajes, ya que la conversación sale cifrada de nuestro celular y solo la persona destinataria que recibe el mensaje puede leerlo.

Característica importante:

Podemos poner un temporizador a los mensajes para que se borren automáticamente un tiempo dado, desde 1 hora hasta 1 semana. Al usar el temporizador desaparecerá el mensaje de ambos dispositivos: de quien manda el mensaje y de quien lo recibe.

Anonimato

Para activar Telegram necesitamos recibir un código de verificación por SMS. Nuestra cuenta de Telegram por tanto está ligada al número al que recibimos este mensaje, que funciona a modo de nombre de usuario.

Una vez instalada la aplicación en nuestros celulares podemos ver quiénes de nuestra lista de contactos usan Telegram y podemos enviarles mensajes cifrados. Esto también significa que cuando queremos comunicarnos con alguien nuevo a través de Telegram necesitamos darle nuestro número de celular.

5. CUIDADOS DIGITALES

5.1 ¿Frente a qué situaciones necesitamos tener cuidados?

Si no queremos dar este número a personas que no conocemos, o no queremos hacerlo público, se puede hacer lo siguiente:

Una opción es instalar Telegram en un celular diferente con un número de celular nuevo que no es el de uso personal.

Otra opción es, al instalar Telegram, pedir que nos envíe el número de verificación en forma hablada a un número de teléfono fijo en lugar de texto SMS.



Tener cuidado con nuestro equipo digital, sea teléfono, computadora o tablet es igual a decir “MEJOR PREVENIR QUE LAMENTAR”. Ya vimos que el mundo de la tecnología digital está en manos de los grandes capitalistas y les sirve para su esquema de dominación. Para ellos, tener acceso a nuestra información personal permite:

Que las empresas extraen nuestra información personal para acosarnos con sus productos, haciendonos caer en la trampa del consumismo.

Que cualquier empresa, gobierno o persona puede tener acceso a nuestros archivos personales, información financiera o información personal. Esto nos hace vulnerables a un ataque o una extorsión.

Que un gobierno de corte represivo que persigue a defensores de derechos humanos nos puede acosar o amenazar cibernéticamente, ubicar donde estamos para hacernos un ataque o extraer información sobre las personas y colectivos con que nos reunimos y actuamos juntos.

Que un agresor y/o acosador sexual puede tener acceso a nuestros fotos personales que subimos a nuestros teléfonos e incluso, puede hacerlas públicas, puede mandarnos mensajes amenazantes u ofensivos y puede ubicarnos geográficamente para saber donde vamos a estar en cierto momento, utilizando esta información para agredirnos físicamente.

5. CUIDADOS DIGITALES

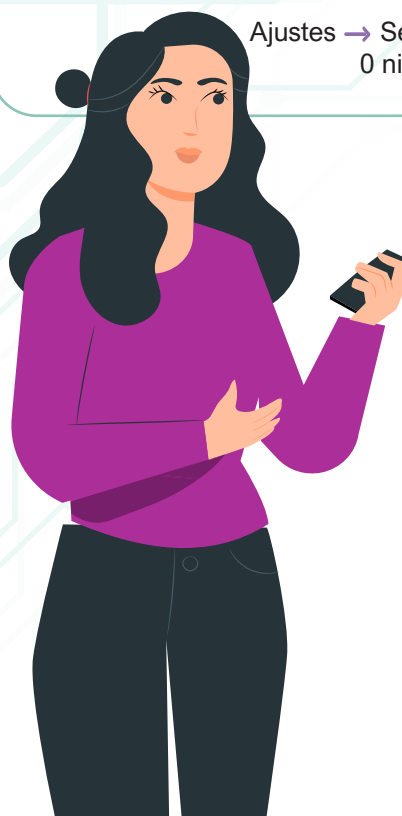
5.2 Protección básica en el uso de celulares.

Ahora tener celular es algo común, la mayoría de personas tenemos un teléfono celular con el cuál nos comunicamos, hacemos llamadas y utilizamos todas las apps disponibles para conectarnos a internet. Es importante cuidar y proteger nuestras comunicaciones, la pérdida de nuestro celular puede ocasionarnos muchos problemas si no sabemos como protegernos de estos riesgos.

¡OJO!

Tenemos que saber que hacer que en caso de que no tengamos celular, elaborar estrategias que siempre contemplen un plan B sin tecnología es la mejor forma de organizarnos, ya que el sistema puede fallar.

Cómo primera medida de seguridad para proteger nuestro celular hay que colocar una contraseña para desbloquear la pantalla.



Ajustes → Seguridad → bloqueo de pantalla.
0 ni patron ni pin

Usa una contraseña de mínimo 10 caracteres por ejemplo la frase:

La pacha mama tiene 13 caracteres contando los espacios, también puedes codificar un poco más la contraseña colocando mayúsculas y números por ejemplo L4 P4ch4 M4m4 en donde sustituimos la A por un 4.

¿Que es un Cifrado y/o Encriptado?

Por ejemplo leemos la siguiente frase:

Un cántaro de rosas

Es una frase que podemos leer fácilmente pero si aplicamos un cifrado y/o encriptado la frase se vería algo así:

mOt3mdvbs\$)%#"lfgq

¿Por qué es importante cifrar y/o encriptar el celular?

En el caso de pérdida o robo del dispositivo, no podrán ingresar a nuestra información, ya que tendrán que formatear el celular para poder utilizarlo nuevamente.

¡ VAMOS A LA PRÁCTICA!

■ Antes de cifrar el celular asegúrate de cumplir con estas condiciones:

- Verificar que el celular tenga la opción de Encriptado y/o Cifrado; y también cifrado de la SD.
- Que el celular tenga un 80% de batería
- Conectar el celular a lared eléctrica.

Para encriptar y/o Cifrar busca en el celular Ajustes → Seguridad → Encriptación y/o Cifrado.

Otras recomendaciones de seguridad:

- 1** Dejar los teléfonos fuera de las reuniones. (Esto se debe a que la mayoría de aplicaciones que utilizamos en nuestros teléfonos nos piden un permiso para acceder a ciertas configuraciones como por ejemplo, fotos de la galería, contactos, micrófono, etc. Y ojo a este último porque esta es una de las razones por las que no debemos tener teléfonos en una reunión de suma importancia, ya que pueden estar interviniendo nuestras líneas cosa que ni aun apagando el teléfono deja de pasar.)• Antes de ir a una concentración acordar un punto de encuentro. • Hacer un respaldo del celular regularmente.
- 2** Eliminar información del celular que no necesitemos.
- 3** **Otras configuraciones de seguridad**
Desactiva el wifi, bluthooth y GPS cuando no los usas.

4 Utiliza un VPN (usa Bitmask u otra) para protegerte cuando uses redes públicas wifi (<https://milpadigital.org/milpadigital-33>).
O mejor aún no utilices redes wifi públicas :).
Usa las aplicaciones de chat y llamadas como Signal (<https://milpadigital.org/milpadigital-6>) o Wire (<https://milpadigital.org/milpadigital-5>) con autodestrucción de mensajes.

5 Utiliza F-droid (<https://milpadigital.org/milpadigital-18>) para instalar aplicaciones sin publicidad y con más seguridad. • Instala el navegador Firefox y configura los complementos de seguridad como Hhttps Everywhere, Ublock Origin y Privacy Badger.

¿CÓMO NOS VIGILAN?

Existen múltiples formas de vigilancia por medio de la tecnología. Al mejor estilo de la saga cinematográfica de Matrix, todo tiene una puerta trasera. Hay diferentes formas en las que pueden darnos seguimiento, algunas específicas y otras genéricas no por eso menos poderosas. Es realmente increíble la información que recopilan gigantes como Facebook, Google o Amazon. Esta capa es la que conocemos como minería de datos, que es una capa más genérica de vigilancia y predicción del comportamiento individual y en masa. Pero además puede existir la vigilancia directa, realizada por personas con conocimientos especializados que son capaces de intervenir nuestras comunicaciones de múltiples maneras:

- Software y equipo de rastreo
- Spyware (malware espía)
- Hardware y software cerrado controlado por transnacionales monopólicas.
- Obligación de aceptar términos y condiciones para usar las apps.
- Con las antenas de telefonía celular cuando hacemos llamadas, mandamos mensajes, registran ubicación, quién llama, quién contesta, hora, duración, etc.

→ <https://milpadigital.org/milpadigital-1>
<https://milpadigital.org/podcast-cosecha-digital-episodio-1>

5.3 Cuidándonos en la red para estar seguras fuera de ella.

Los datos y la información que generamos con nuestro uso de internet les interesan por diferentes motivos a gobiernos, empresas de telecomunicaciones, empresas privadas comerciales, empresas tecnológicas de alto rendimiento (Facebook, Amazon, Apple, Netflix

y Google), hackers maliciosos (porque también los hay con buenas intenciones), o incluso una expareja que nos acose.

En el mundo digitalizado de hoy en día, las consecuencias de generar datos continuamente no siempre son fáciles de prever, así que lo aconsejable es intentar tener el mayor control posible sobre lo que hacemos público y lo que queremos mantener privado.

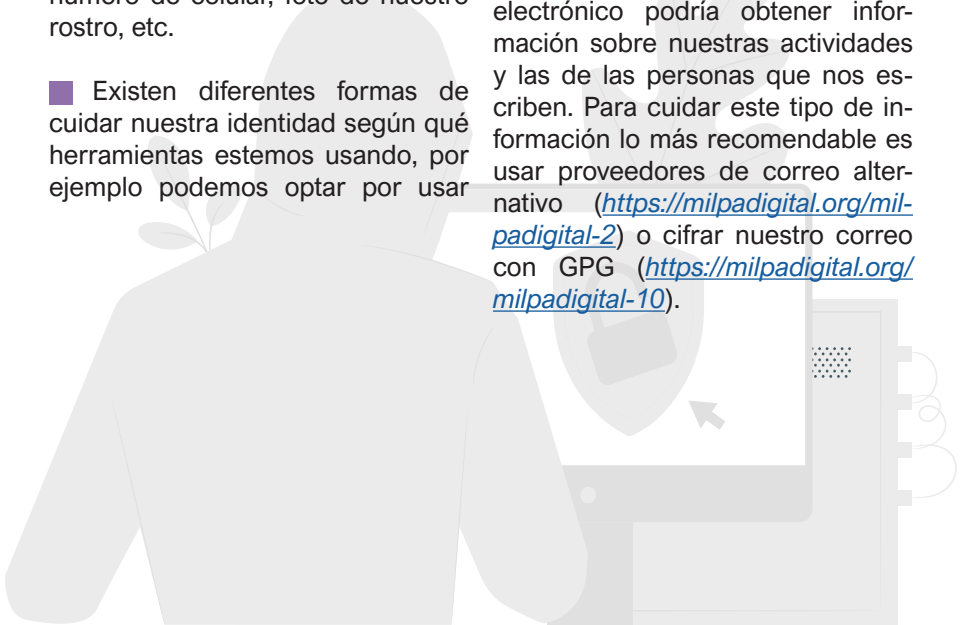
CUIDAR NUESTRA IDENTIDAD EN INTERNET ES AÚN MÁS IMPORTANTE SI SOMOS ACTIVISTAS O MILITANTES DE ALGUNA CAUSA.

Nuestra identidad es uno de los tesoros más grandes que cuidar en internet. Debemos considerar sensible y privado cualquier dato que permita identificarnos, por ejemplo nuestro nombre, apellido, dirección, número de identidad, número de celular, foto de nuestro rostro, etc.

■ Existen diferentes formas de cuidar nuestra identidad según qué herramientas estemos usando, por ejemplo podemos optar por usar

seudónimos en redes sociales que lo permitan (por este motivo no es recomendable usar Facebook), usar aplicaciones de mensajería orientadas a cuidar nuestra privacidad como Signal (<https://milpadigital.org/milpadigital-6>), Tor (<https://milpadigital.org/milpadigital-8>) y una VPN (<https://milpadigital.org/milpadigital-33>), y obtener consenso por escrito antes de subir fotos a redes sociales, si las personas no quieren que sus rostros sean públicos, podemos usar Obscurecam (<https://milpadigital.org/milpadigital-36>) para difuminarlos.

■ De la misma forma en que protegemos nuestra identidad, también debemos cuidar la identidad de les compañeres con quienes nos comunicamos y la información que intercambiamos con ellos. Para esto es imprescindible tener contraseñas fuertes y difíciles de adivinar (<https://milpadigital.org/milpadigital-7>), ya que si alguien tuviera acceso a nuestra cuenta de correo electrónico podría obtener información sobre nuestras actividades y las de las personas que nos escriben. Para cuidar este tipo de información lo más recomendable es usar proveedores de correo alternativo (<https://milpadigital.org/milpadigital-2>) o cifrar nuestro correo con GPG (<https://milpadigital.org/milpadigital-10>).



Para proteger la información que tenemos guardada en nuestras computadoras podemos cifrar nuestro disco duro o una carpeta dentro de nuestro sistema operativo con Veracrypt (<https://milpadigital.org/milpadigital-34>)

■ Para proteger la información que tenemos guardada en nuestras computadoras podemos cifrar nuestro disco duro o una carpeta dentro de nuestro sistema operativo con Veracrypt (<https://milpadigital.org/milpadigital-34>.)

■ Otro cuidado básico a tener en cuenta es no abrir links o enlaces ni descargar archivos adjuntos que recibamos por correo electrónico o mensajería (<https://milpadigital.org/milpadigital-9>) ya que podríamos estar dando acceso a una tercera persona a nuestro dispositivo y a toda la información que guardamos en él. Para protegernos de este tipo de ataques podemos confirmar por otro medio con la persona que nos envió el mensaje (si es una persona desconocida o el enlace viene de un mensaje automático, nunca hacer clic ni descargarlo), también podemos instalar un antivirus (<https://milpadigital.org/milpadigital-35>). En el caso de nuestras computadoras podemos migrar a un sistema operativo de código libre como Ubuntu (<https://milpadigital.org/milpadigital-17>) o Debian (<https://milpadigital.org/milpadigital-18>) que son más seguros porque un gran número

de personas están revisándolos y actualizándolos constantemente gracias a que su licencia lo permite.

■ Otra estrategia de cuidados básicos es hacer copias de seguridad cada cierto tiempo dependiendo de cuanta información nueva generemos y qué tan sensible sea. Debemos guardarla en dos lugares diferentes (disco duro y USB), por ejemplo tener una copia de seguridad en un USB que llevamos en nuestra mochila junto con nuestra computadora es una mala práctica, ya que si perdemos la mochila perderemos los dos dispositivos.

■ No todas las estrategias de cuidados digitales tienen que ver con escoger herramientas más seguras o cifrar nuestro correo electrónico o computadora. Cuidarnos implica cosas tan sencillas como asegurarnos que no haya nadie que pueda ver cuando escribimos nuestra contraseña, o incluso tener cuidado de que nos roben nuestro teléfono o nuestra computadora.

La seguridad digital no es un producto, sino un proceso. Lo mejor es aprender de a poco y no tener miedo ni flojera de usar herramientas nuevas. Es útil hablar con otros compañeros sobre este tema, compartir dudas y buscar soluciones y alternativas juntas.

<https://milpadigital.org/milpadigital-4>

<https://milpa.digital.org/podcast-cosecha-digital-episodio2>



5.4 Podcast 9 Riesgos y Amenazas

Escucha el programa radial aquí:

<https://milpadigital.org/podcast-cosecha-digital-episodio9>

6. HERRAMIENTAS LIBRES Y SEGURAS

Esta es una lista de herramientas alternativas de los grandes monopolios de la tecnología, desde una perspectiva de las tecnologías de genero.

Mensajería Instantánea Celular

Signal: Android, iOS Mensajes y llamadas encriptadas, desvanecimiento de mensajes en grupos, seguridad en grupos.

Wire: Android, iOS, Mensajería Segura

Correo electrónico

Riseup.net: Necesitas tener un código de invitación ProntoMail.

Cuenta de correo alternativa

K9Mail: Android – Cliente de correo alternativo para no usar gmail

Thunderbird: Cliente de correo para la computadora.

Navegación Segura y Anónima

Firefox: Navegador para la computadora y el celular, es importante instalar complementos de seguridad.

Bitmask: VPN Navegación segura disponible para el celular y la computadora

Orbot: TOR para el celular y también en modo VPN.

TOR Browser: TOR para la computadora.

Nube con NextCloud

Nextcloud: Almacenamiento de archivos y datos de forma segura y edición colaborativa de documentos en línea, Calendario Sincronizado y Respaldo de Directorio de Contactos y más. Si quieres una nube puedes escribir a CódigoSur. También puedes usar la nube de Nextcloud con <https://disroot.org/>

Otras herramientas útiles

F-DROID: Es un catálogo instalable de aplicaciones de software libre para Android descargar de <https://f-droid.org/>

Video Conferencia

Jitsi - <https://meet.jit.si/>

Organizador

<https://framadate.org/>

Mapas libres

OsmAnd

OpenStreetMap

Visualización de datos en un mapa

Umap

Guardar y crear contraseñas

Keepass

Redes Sociales alternativas

Mastodon

<https://esquite.mazorca.org/> y
<https://systemserver.town/>

CrabGrass

<https://crabgrass.riseup.net/>

PatchWork

<https://www.scuttlebutt.nz/>

Más redes sociales alternativas:

Face Slim App

Alternativa a la aplicación de facebook y no contiene publicidad.

Twidere App

Alternativa a Twitter y no contiene publicidad, configuratus cuentas de Twitter y Mastodon en ella.

NewPipe

Alternativa a Youtube no contiene publicidad, mantiene la opción de reproducción de video en segundo plano. No se puede ver streaming en vivo.

Antivirus, Malware y virus

Avira *, AVG, Avast

Anti-virus para Android & iOS y computadoras

<https://virustotal.org>

Aquí puedes verificar si un enlace o documento contiene algun tipo de virus, malware o contenido malicioso.

En caso de robo

Prey

Cuando el celular ha sido robado se puede pagar para hacer un borrado remoto

Android Lost

Borrado remoto para Android <http://www.androidlost.com> o por msn.

Sistema Operativo / Software Libre para Celulares

LinageOS - <https://wiki.lineageos.org/devices/>

Para Radio Online

Broadcastmyself

Transmisión de radio por internet desde el celular

Mixxx o Butt para la computadora.

Herramientas para la defensa y protección

<https://acoso.online>

Herramienta ante la publicación no consentida de imágenes y videos íntimos por medios electrónicos es una forma de violencia de género contra las mujeres heterosexuales y personas LGBTIQ.

<https://actua.karisma.org.co/alertamachitroll/>

Machitroll Se trata de una especie de cibernauta que se caracteriza por el impulso feroz de atacar a otras personas usando comentarios, gif e imágenes violentas en la web cada vez que encuentra contenidos feministas en internet. Puedes levantar alertas y poner sellos según la especie de machitroll.

<https://myshadow.org/es>

Cuando estos se juntan y permiten crear perfiles sobre nosotras, se convierten en nuestra sombra digital.

<https://securityinbox.org/es/guide/social-networking/>

Protegete cuando utilices redes sociales, muchos ataques pueden pasar, suplantación de identidad etc.

<https://www.codingrights.org/safernudes/>

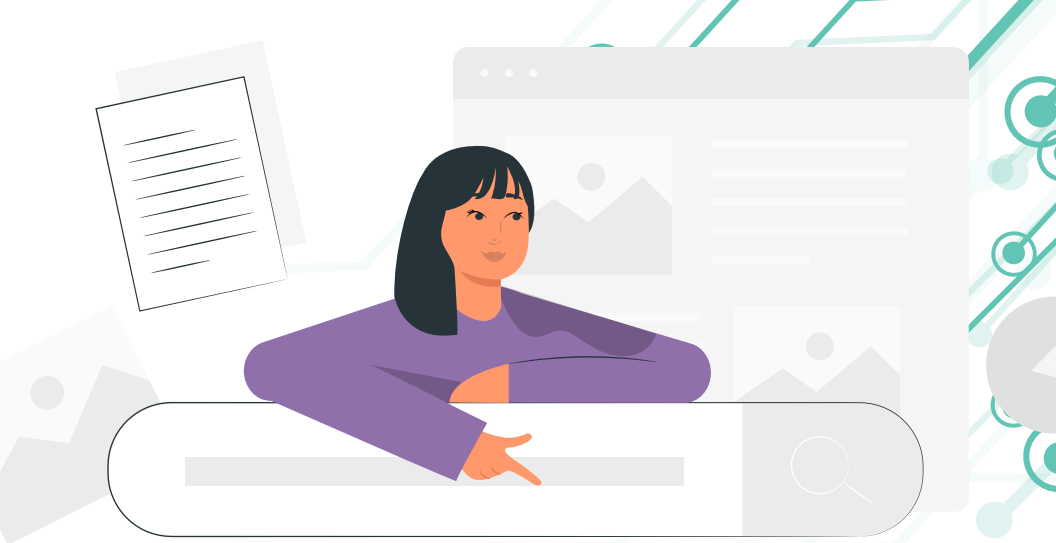
Sexting seguro, derecho a la sexualidad y privacidad

7. FIREFOX:

Mozilla Firefox es un navegador libre de código abierto, desarrollado para Linux, Android, IOS, OS X, Microsoft Windows. Si todavía no lo tienes instalado, puedes hacerlo en este momento desde tu computadora o teléfono celular.

La privacidad es una de las principales razones por las cuales recomendamos el uso de Firefox como navegador. No tenemos que olvidarnos de que Google basa su negocio en la publicidad y que para ello debe hacer una recolección de todos nuestros datos. Si no nos gusta que Google siga haciendo más dinero con nuestros datos usemos Firefox configuremos las funciones como decirle a las webs que no nos rastreen, incluye el buscador DuckDuckGo por defecto y nos da la opción de no enviar datos de uso si no queremos y muchas más opciones, solo ve al menú y en preferencias buscas la viñeta seguridad y también en Privacidad.

Para finalizar solo mencionar que de los navegadores de internet que derivan de Firefox esta Tor Browser que utiliza la red TOR para tener anonimato en la red y acceder a contenidos en la Deep Web. Para instalarlo entra a <http://torproject.org/>.



¿Qué son los complementos para el navegador?

Un complemento es como una aplicación para el navegador.

Hay dos tipos de complementos: extensiones, que añaden funcionalidad; y temas, que cambian cómo se ve el navegador.

Con las extensiones podemos agregar funciones a Firefox para navegar más rápido, más seguras, hacerlo más fácil o más divertido.

¿De dónde las Instalamos?

Cuando instalamos programas es muy importante verificar el origen del que descargamos algo. Si no es un sitio confiable, puede que el programa nos acabe perjudicando. En este caso, la comunidad del Navegador Firefox hace una revisión de calidad para asegurar que las extensiones publicitadas en su sitio web son fiables.

■ Vamos a <https://addons.mozilla.org/es/firefox/> y buscamos el complemento o el tema que queremos instalar.

■ Después de leer la descripción y la valoración de la comunidad, hacemos clic en el botón de “instalar.”

¿Cuándo instalar un complemento?

Instalar una extensión toma muy poco tiempo. La extensión baja automáticamente unos archivos que se instalan y se quedan en nuestro disco duro. Así que es una buena idea instalar nuestros complementos preferidos cuando estamos en una computadora que vamos a usar con frecuencia. Además, instalar un complemento es una de las formas más sencillas de hacer algo para mejorar nuestra protección en línea.

COMPLEMENTOS PARA USO BÁSICO:

HTTPS Everywhere

Forzar las páginas seguras con https. <https://www.eff.org/https-everywhere>

Privacy Badger - bloquea la publicidad que espía. <https://www.eff.org/privacybadger>

Self-destructing cookies

Destruye las (cookies = la información enviada por un sitio web y almacenada en el navegador, así el sitio web puede revisar tu navegación anterior). <https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/>

Ublock Origin

Bloquea la publicidad de las páginas y evita su descarga, haciendo una navegación más rápida y segura. <https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/> HTML5 Alto performance para ver vídeos en la web. <https://addons.mozilla.org/en-US/firefox/addon/html5-video-everywhere/>

DuckDuckGo

Buscador alternativa a Google. <https://addons.mozilla.org/en-US/firefox/addon/duckduckgo-for-firefox/>

INSTALA ESTOS OTROS COMPLEMENTOS CUANDO TE ACOSTUMBRES A LOS PRIMEROS DE LA LISTA:

■ NoScript

Sólo permite JavaScript, Java y otros plugins en los sitios web de confianza.

■ Para Chrome instalar Umatrix es un equivalente. <https://noscript.net/getit>

■ Canvas Blocker

Bloquea JS-API <https://addons.mozilla.org/en-US/firefox/addon/canvasblocker/>

■ Open With

Menús y pestañas para abrir la página en otro navegador <https://addons.mozilla.org/es/firefox/addon/open-with/>

■ User Agent Switcher - Sustituir al agente de usuario del navegador.

■ <https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher-firefox/>

Escucha:

<https://milpadigital.org/milpadigital-15>

<https://milpadigital.org/podcast-cosecha-digital-episodio4>

8. PODCAST SOBRE TECNOLOGÍAS

Hacer un listado de podcast sobre tecnología.



Capítulo

Redes sociales y sus cuidados

Apps seguras y libres

Tails: Conectándonos a internet de manera segura y anónima

Mastodon: la red social libre y descentralizada

Con F-droid te liberas de las tiendas privadas

K-9 Mail una app alternativa para revisar correo en el celular

Navegar con Firefox y sus complementos

Chats Seguros y cifrados con Signal

Usando proveedoras de correos electrónicos alternativos

Haciendo llamadas con Mumble voz libres y segurase

Mensajería y llamadas con Wire

Difuminación de caras en fotos y videos con ObscuraCam

Evadir la censura y la vigilancia con el navegador TOR

Cuidándonos en la red para estar seguras

Haz clic en el capítulo para escuchar el programa en Archive.

9. DENUNCIA DIGITAL



Denunciar violaciones de los derechos humanos de las mujeres es una tarea importantísima para nosotras como defensoras.

Hay distintos tipos de denuncias que debemos realizar:

1. Denuncias de violaciones de derechos colectivos, por ejemplo cuando hay una violación de los derechos económicos de las mujeres que laboran en cierta empresa y reciben un menor salario de los hombres o cuando una empresa utiliza publicidad que agrede la dignidad de las mujeres en general.

2. Violaciones de los derechos individuales de una mujer. Esto pasa cuando una mujer es objeto del acoso o abuso sexual, emocional o

psicológico, físico, económico y/o patrimonial. En los dos casos, la denuncia puede ser escrita, en un podcast o en video.

Unos consejos para la denuncia de violaciones de derechos colectivos:

- Realizar la denuncia en nombre de una organización
- Analizar la situación por denunciar entre el grupo de compañeras.
- Identificar con las compañeras qué resultado esperamos tener de nuestra denuncia, esto nos ayudará a decidir sobre el contenido y el formato. También identificar posibles riesgos que nos puede implicar para buscar mitigarlos.
- Decidir qué nivel de anonimato queremos guardar para las personas que den su testimonio, especialmente si el formato es un video. ¿Queremos poner el nombre y lugar de residencia de las mujeres que hablan o no? ¿Queremos que salga su rostro o no?.

Unos consejos para la denuncia de violaciones de derechos individuales:

- Buscar ayuda psicológica antes de poner la denuncia.
- Hacerte acompañar por una amiga y/o defensora.

- Poner la denuncia en las instancias jurídicas antes de realizar la denuncia en redes sociales.
- Identificar con la psicóloga, con una amiga o con una defensora qué resultado esperamos tener de nuestra denuncia en redes sociales, esto nos ayudará a decidir sobre el contenido y el formato. También es importante identificar posibles riesgos que nos puede generar, para buscar mitigarlos.
- Decidir qué nivel de anonimato queremos guardar. ¿Queremos que vaya el nombre de la persona agredida o no? ¿Pondremos el nombre del agresor? ¿Quiero que vaya mi rostro?

En los dos casos es importantísimo garantizar la veracidad de la denuncia, para no caer en el mal uso de las redes sociales.

En algunos países los movimientos de mujeres han desarrollado sistemas de denuncia en redes sociales en donde se han expuesto a agresores con consecuencias hasta legales, que en tiempos sin redes ni siquiera se visibilizaba, Es una herramienta importante que nos ayudará a ampliar el alcance de nuestro trabajo.

10. BÚSQUEDA DE INFORMACIÓN PENDIENTE

El internet es un excelente recurso para buscar información sobre un tema, para encontrar otras organizaciones con quienes podemos coordinar el trabajo o para buscar apoyo en una emergencia. Pero como el internet nos puede ayudar, también nos puede afectar. Por que en internet, cualquiera publica sus cosas, no solo personas u organizaciones que comparten nuestros valores, enfoques, preocupaciones e intereses. No hay garantía que la información que encontramos en internet es verdad, depende de quién lo escribe y para qué lo escriben.

Por esto, es bueno buscar información en páginas conocidas, con reconocido valor y si es posible, con reconocidas autoras. A continuación encontrarán una serie de recomendaciones de páginas que les puede servir en su trabajo.



NÚMEROS, CONTACTOS Y FONDOS DE EMERGENCIA

- Listado de números de emergencia
Bomberos: *198
Cruz Roja: *195
Policía: *911
COPECO: *113

LISTADO DE AUTORIDADES PARA DIRIGIR UNA PETICIÓN

Autoridades en Tegucigalpa, Honduras

- **Presidencia de la República.** Casa Presidencial, Boulevard Juan Pablo II. Tel: 2290-5000. Correo-e: info@presidencia.gob.hn
- **Secretaría de Derechos Humanos,** Justicia, Gobernación y Descentralización. Boulevard Centroamérica, contiguo al INPREMA, 4to y 5to piso. Tel: 2232-8900/2232 6800 ext. 1164. Correo-e: transparencia@sdhjgd.gob.hn
- **Secretaría de Estado en el Despacho de Seguridad.** Plantel Casamata, subida al Picacho. Tel: 2220-5547/2220-4553. Fax: 2237-9070.
- **Fiscalía General de la República.** Colonia Lomas del Guijarro, Edificio Lomas Plaza II, Avenida República Dominicana. Tel: 2221-8215. Fax: 2221-3099
- **Fiscalía Especial de Derechos Humanos y Fiscalía Especial de la Mujer.** Tel: 2221-5620 (teléfono general para todas las fiscalías especiales).
- **Procuraduría General de la República.** Lomas del Guijarro Sur, Boulevard San Juan Bosco, Edificio Centauro. Tel: 2235-6100/2235-6095. Fax: 2239-6182. Correo-e: pgrdespacho@pgrhonduras.gob.hn

- ❑ **Comisionado Nacional de los Derechos Humanos.** Colonia Florencia Norte, Boulevard Suyapa, contiguo banco Lafise. Telefax: 2231-0882/2235-7697/2235-3532. Correo-e: central@conadeh.hn
- ❑ **Presidencia de la Corte Suprema de Justicia.** Palacio de Justicia, Centro Cívico Gubernamental. Boulevard Fuerzas Armadas. Tel: 2275-3181 al 85. Correo- e: comunicaciones@poderjudicial.gob.hn
- ❑ **Oficina de la OEA en Honduras.** Edificio Corporativo Guijarros, Col. Lomas del Guijarro Sur, Bloque W, Avenida Berlín. Tel: 2239-9530/2239-9471. Correo-e: OASHonduras@oas.org
- ❑ **Oficina del Alto Comisionado para los Derechos Humanos en Honduras.** Casa de las Naciones Unidas. Avenida República de Panamá, Colonia Palmira. Tel: 2220-1100. Correo-e: onuddhh@ohchr.org
- ❑ **Sistema Nacional de Protección de para las y los Defensores de Derechos Humanos, Periodistas, Comunicadores Sociales y Operadores de la Justicia.** Colonia Florencia Norte, Boulevard Suyapa, Casa #211. Tel: 2235-8650. Número de emergencia para horas inhábiles: 9874-8595. Correo-e: recepcioncasosdgp@gmail.com
- ❑ **Instituto Nacional de la Mujer.** En el 6to y 7mo piso del Edificio de Banadesa, en el Barrio Concepción, 13 y 14 calle, entre 4ta y 5ta Avenida de Comayagüela. Tel: 2290-7300. Correo-e: secretariapresidencia@inam.gob.hn • Secretaría de Relaciones Exteriores y Cooperación Internacional. Avenida Juan Ramón Molina, 1ra Calle, 7ma Avenida, Antiguo Edificio del Banco Central, Barrio El Centro. Tel: 2236-0300. Correo-e: cancilleria.honduras@gmail.com



AUTORIDADES EN EL EXTRANJERO

- ❑ **Misión Permanente de Honduras ante las Naciones Unidas en Ginebra.** Tel: +41 227-100-760. Fax: +41 227-100-766. Correo-e: mission@hondurasginebra.ch
- ❑ **Embajada de Honduras en Bruselas.** Tel: +32 2734-0000/+32 2734-7027. Fax: +32 2735-2626. Correo-e: info@hondurasembassy.be
- ❑ **Embajada de Honduras en la OEA.** Tel: 001 202-244-5653/001 202-244-5430. Correo-e: honduras@oas.org

10.1 DIRECTORIO DE ORGANIZACIONES

Guía de Organizaciones de Derechos Humanos

- ❑ **CDM Centro De Derecho Mujeres**
Col Lara Norte, Calle Lara Casa No.834
Tegucigalpa 4562, Teg. HN
<https://derechosdelamujer.org>
- ❑ **COIPRODEN**
Tegucigalpa Distrito Central, 11101
Karen Andino 3273-0729
<https://redcoiproden.org/>
- ❑ **ASONOG**
Santa Rosa de Copán
+504 2662-2626
<http://www.asonog.hn/>
- ❑ **CEM-H Centros De Estudios De La Mujer**
Colonia Ruben Dario, 1ra. Avenida, Calle
Palermo, Tegucigalpa
2239-8979
- ❑ **Foro De Mujeres Por La Vida**
San Pedro Sula , Cortes
Llamar 3287-7729

- **COFADEH Comité De Familiares Desaparecidos De Honduras**
Casa 1301, Barrio La Plazuela, Tegucigalpa
+504 2220-5280
+504 2220-7147

- **CIPRODEH Centro De investigación Y Promoción De Los Derechos Humanos**
Apartado Postal 3829
Tegucigalpa
+504 2232 3572
+504 2232 0857
+504 2232-3519
+504 2232 3553

- **INAM Instituto Nacional De La Mujer**
En el 6to y 7mo piso del Edificio de Banadesa,
Barrio Concepción, 13 y 14 calle, entre 4ta y 5ta
Avenida de Comayagüela, Francisco Morazán
+ (504) 2220-0906, (504) 2220-0852, (504)
2220-0902

- **Movimiento de Mujeres por la Paz “Visitación Padilla” Tegucigalpa Honduras**
(504) 222 7779

- **OFRANEH Organización Fraternal Negra De Honduras**
<http://ofraneh.org/>

- **Red Nacional De Defensoras De Derechos Humanos En Honduras**
<https://im-defensoras.org/red-nacional-de-defensoras-de-derechos-humanos-en-honduras/>

- **CONADEH**
Oficina Central Colonia Florencia Norte,
Boulevard Suyapa, Contiguo a banco Lafise
Tegucigalpa,
Honduras C.A.. Telefax: 2231-0204, 2231-0882,
2235-7697,

10.2 BASE DE DATOS

Consulta más información a través de estos sitios electrónicos.

ORG.	CONTENIDO	CONTACTO	URL
CDM	Infografía sobre femicidios realizados en honduras en 2022		https://derechosdelamujer.org/project/infografias-2022/
CDM	Boletín: violencia contra las mujeres en honduras 2019-2020		https://derechosdelamujer.org/wp-content/uploads/2021/08/Boletin_VCM2019-2020.pdf
CDM	¿Qué hacer? – Ciberviolencia		https://derechosdelamujer.org/que-hacer-ciberviolencia/
Ciudad Mujer	Estos son los servicios que te ofrecemos en Ciudad Mujer	info@ciudadmujer.gob.hn	https://www.ciudadmujer.gob.hn/servicios/
Ciudad Mujer	Todo lo referente a Ciudad Mujer	+504 9739 6698 info@ciudadmujer.gob.hn	https://www.ciudadmujer.gob.hn/
CEMH	Todo lo referente a CEMH	cemhhonduras@yahoo.es +504 2239-897	http://www.cemh.org.hn/contact/
CESPAD	Estudios sobre Realidad Nacional: defensa Recursos naturales, el tema de Mujeres, Democracia, corrupción	contacto@cespad.org.hn	https://cespad.org.hn/
ONU MUJERES	Derechos de las mujeres		https://www.unwomen.org/es
PNUD	Objetivos de desarrollo sostenible		https://www.hn.undp.org/
CEHPRO-DEC	desarrollo comunitario y la solidaridad local nacional e internacional a partir de la organización		https://cehprodechn.org/ FB: Cehprodec TW: @cehprodec INSTA: @cehprodec
ERIC sj	Realidad Nacional		https://eric-sj.org/

ORG.	CONTENIDO	CONTACTO	URL
COIPRO-DEN	Biblioteca Digital de COIPRO-DEN	Dennis Salgado 3273-0729	https://redcoiproduen.org/biblioteca/
Casa Alianza	Informe Mensual de la Situación de los Derechos de las Niñas, Niños y Jóvenes en Honduras, marzo del 2022	Jaime Flores 9484 – 9860	http://casa-alianza.org.hn
DINAF	Página oficial		https://dinaf.gob.hn/
Secretaría de Derechos Humanos	Página oficial Sistema de Monitoreo de Recomendaciones de Honduras (SIMOREH)		https://www.sedh.gob.hn/ https://simoreh.sedh.gob.hn/buscador/home
Secretaría de Derechos Humanos	Sistema de Monitoreo de Recomendaciones de Honduras (SIMOREH)		https://simoreh.sedh.gob.hn/buscador/home



10.3 BIBLIOGRAFÍA DIGITAL

Guías y materiales

- ❑ <https://escuelafeminista.red/material/guiaprotecciondigital.pdf>
- ❑ <https://cyborgfeminista.tedic.org/recursos/>
- ❑ <https://ciberseguras.org/materiales/>
- ❑ <https://ciberseguras.org/materiales/>
- ❑ <https://web.karisma.org.co/recurso-descargable-violenciadigitaldegenero/>

Guía producida por:

Barracón Digital



El Barracón Digital es un hacklab tekno-cultural, un espacio seguro para las personas activistas donde se comparte y lucha por los derechos humanos y los derechos digitales. Desde ahí realizan actividades tecnológicas, culturales, talleres, co-working e intercambios de conocimientos. Un universo de temas sobre feminismos, software libre, cultura libre, podcast, ciberactivismo, permacultura, protección digital, radio, vídeo e intercambio de semillas .

