en-
tra ma da
FEMI-
NISTA

ENCUENTRO DE
CIBERFEMINISMO

NUESTROS MANTRAS

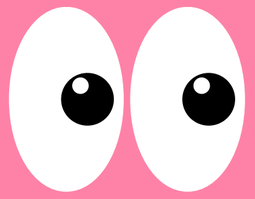
1- Aprender entre todes, escucharnos y respetar la palabra, todes podemos aportar al intercambio

2- Generar un espacio de confianza y seguro entre todes

3- Generar acuerdos de registro

4- Disfrutar del encuentro

¿CÓMO NOS IMAGINAMOS UNA INTERNET FEMINISTA?



PRINCIPIOS (17) FEMINISTAS PARA INTERNET

Acceso:
a internet
a la información
al uso de tecnología

Expresión:
amplificación del discurso
libertad de expresión
pornografía y contenidos ofensivos

Movimientos y participación pública:
resistencias
construcción de movimientos
toma de decisiones en la gobernanza de internet

Agencia:
consentimiento
privacidad y datos
anonimato
violencia en línea

- **¿cómo podemos “diseñar presencias apropiadas” que refuercen nuestra habilidad para comunicar y trabajar de manera segura cuando estamos conectadas?**

- **¿cómo podemos de manera colaborativa “crear espacios seguros” (conectados o físicos) que permitan a nuestras comunidades compartir, comunicar y crecer?**

el feminismo encontró en la internet una aliada para "hackear el patriarcado"

“El movimiento feminista tiene mucho que ver con la forma rizomática de nodos autónomos pero interconectados, con intereses específicos marcados por las diversas agendas pero compartiendo valores y principios comunes”

“para lograr tener masa crítica para incorporar la lucha contra el patriarcado a las nuevas dinámicas de cambio que se están generando en todo el planeta. La capacidad colectiva de apropiación de herramientas digitales para la acción colectiva es imprescindible”

tensión entre las posibilidades libertadoras de internet para el movimiento feminista y la expansión de la vigilancia a través de variados dispositivos y usos tecnológicos como una forma de violencia. Este es un tipo de violencia sutil, tanto es así que llega a parecer invisible en la vida cotidiana. Por eso es necesario enlazar la violencia en ambientes digitales y las discusiones sobre privacidad y derecho a la intimidad en internet

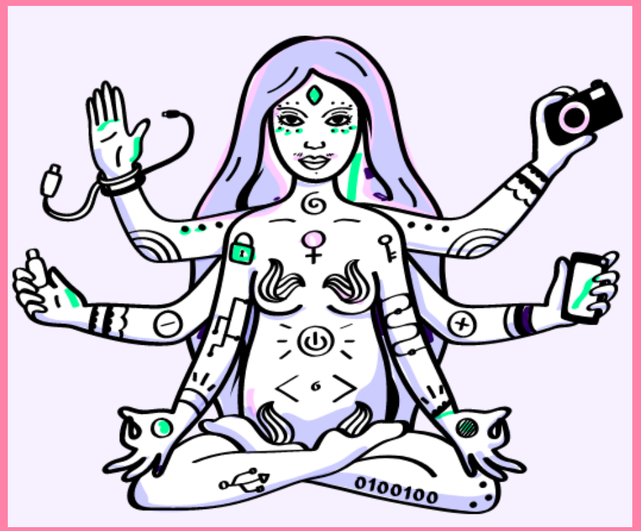
Queres saber más...

https://www.apc.org/es/pubs/principios-feministas-para-internet-version-2

https://www.genderit.org/es/articles/imaginemos-una-internet-feminista-parte-1

https://www.genderit.org/es/articles/imaginemos-una-internet-feminista-parte-2

https://www.genderit.org/es/articles/imaginemos-una-internet-feminista-parte-3



VIOLENCIA DE GÉNERO EN LÍNEA

#1

Definición

Tipos

Efectos

¿QUÉ ES LA VIOLENCIA DE GÉNERO EN LÍNEA?

La **violencia de género digital, o en línea,** refiere a actos de violencia de género cometidos instigados o agravados, en parte o totalmente, por el uso de las **Tecnologías de la Información y la Comunicación (TIC),** plataformas de redes sociales y correo electrónico.

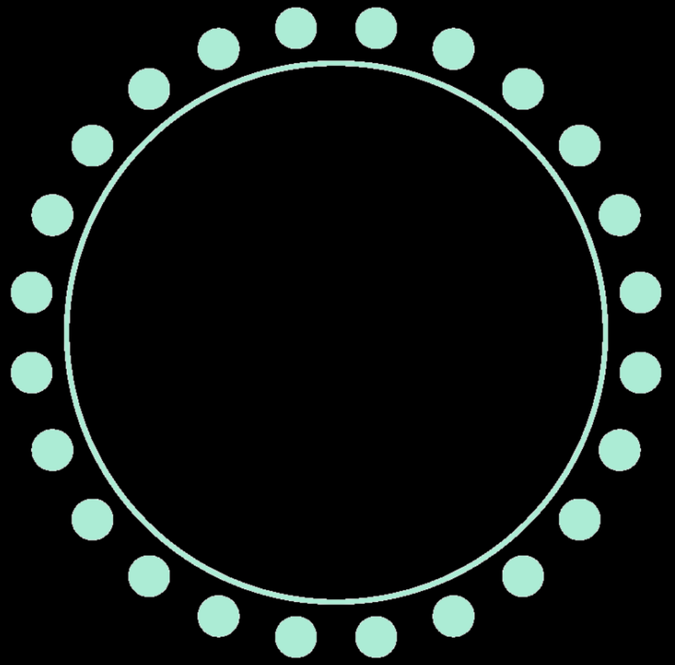
Esta violencia está en constante **interacción** con otros mecanismos de exclusión social como la discriminación por orientación sexual, raza, identidad étnica, opinión política, entre otros factores identitarios, afectando principalmente a mujeres y personas LGBTIQ+ que existen en la intesección de diversos sistemas de opresión alrededor del mundo.

¿La violencia digital es diferente que la violencia física?

¿Por qué?

TIEMPO

En cualquier momento



ANONIMATO

INDIVIDUAL/COLECTIVA

TROLEO

CONTROL Y MANIPULACIÓN DE INFORMACIÓN

PHISHING

DICKPIC

GROOMING

DOXXING

ACCESO Y CONTROL NO AUTORIZADO

Difusión de imágenes

AMENAZAS

TROLEO:
Acto deliberado en Internet realizado por un usuario - anónimo y conocido como troll.-
Los trolls son usuarios que hacen uso de las redes sociales para continuamente contactar, fastidiar, amenazar, y/o asustar y su comportamiento no es un incidente aislado si no que es

DOXXING:
Forma de vigilancia mediante el rastreo profundo de la información disponible en Internet de una persona para su posterior publicación como una forma de intimidación o acoso

Difusión de imágenes no consentidas:
Uso de imágenes íntimas o información personal como una forma de coerción para la explotación o el chantaje sexual.

Phishing:
Mensajes engañosos enviados a un dispositivo para infectarlo con un software espía y poder vigilar o robar sus comunicaciones o información.

DICKPIC (foto de pene no solicitada)

Envío de una foto de los genitales masculinos a una mujer que no lo pidió, es una forma de acoso sexual digital

GROOMING:
Uso de redes sociales para cultivar deliberadamente una conexión emocional con menores de edad con fines de abuso o explotación sexual

13 formas de violencia en línea

Acceso o control no autorizado

Ataques o reestricción de acceso a las cuentas o dispositivos de una persona

Control y manipulación de la información

Robo, obtención, pérdida de control o modificación de información no consentida

Suplantación y robo de identidad

Uso o falsificación de la identidad de una persona sin su consentimiento

Monitoreo y acecho

Vigilancia constante a la vida en línea de una persona

Expresiones discriminatorias

Discurso contra mujeres y personas no binarias que refleja patrones culturales machistas basados en roles tradicionales

Acoso

Conductas de carácter reiterado y no solicitado que resultan molestas, perturbadoras o intimidantes

13 formas de violencia en línea

Amenazas

Contenidos violentos, lascivos o agresivos que manifiestan una intención de daño a alguien, a sus seres queridos o bienes

Difusión de información personal o íntima

Compartir o publicar sin consentimiento algún tipo de información, datos o información privada que afecte a una persona

Extorsión

Obligar a una persona aseguir la voluntad o peticiones de un tercero por poseer algo de valor para ella como puede ser información personal

Desprestigio

Descalificación de la trayectoria, credibilidad o imagen pública de una persona a través de la exposición de información falsa, manipulada o fuera de contexto

Abuso sexual relacionado con la tecnología

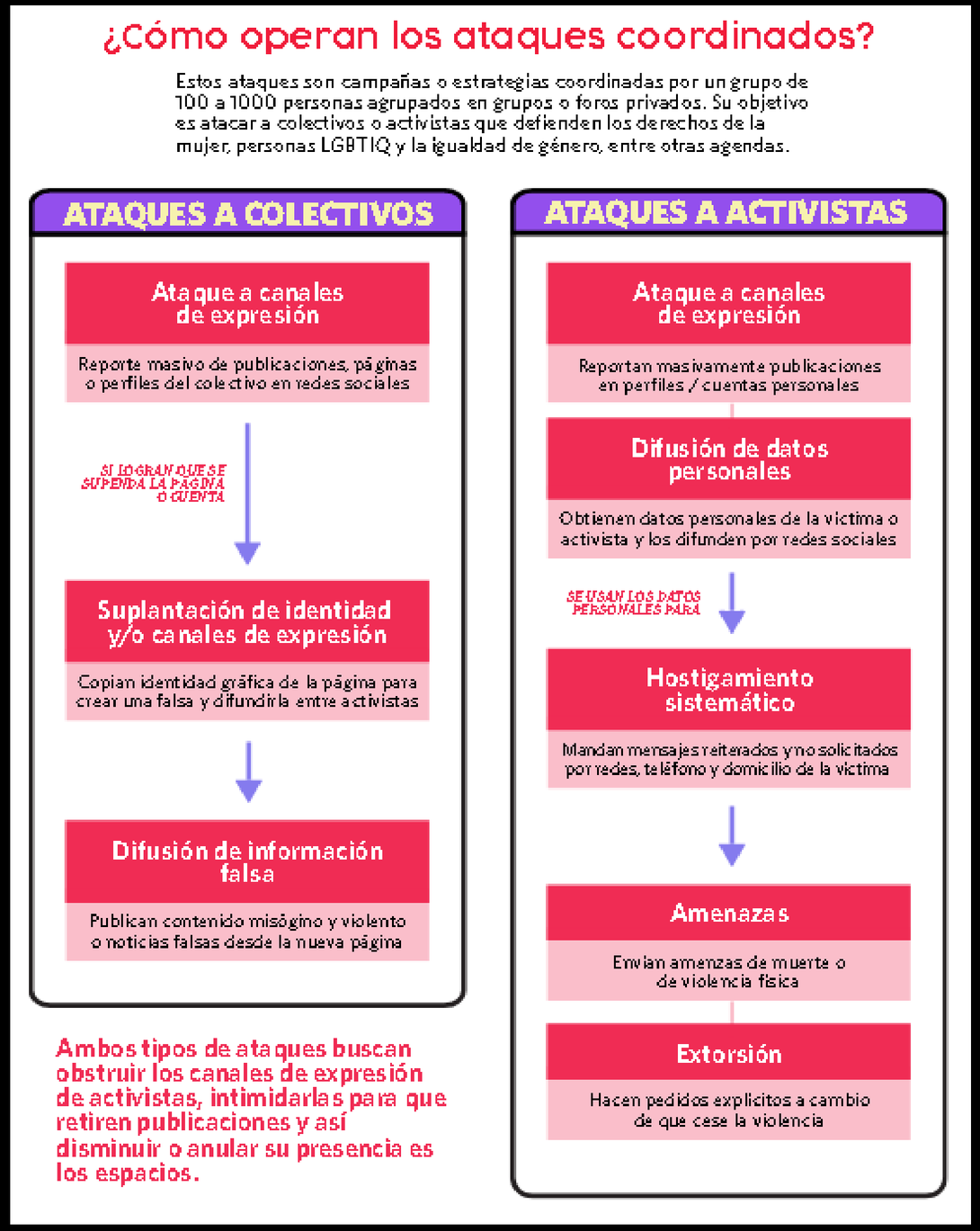
Ejercicio de poder sobre una persona a partir de la explotación sexual de su imagen y/o cuerpo contra su voluntad, puede implicar la obtención de un beneficio lucrativo o de otro tipo

Afectaciones a canales de expresión

Tácticas o acciones deliberadas para tirar y dejar fuera de circulación canales de comunicación o expresión de una persona o un grupo

Omisiones por parte de actores con poder regulatorio

Falta de interés, reconocimiento, acción o menosprecio por parte de autoridades, intermediarios de internet, instituciones o comunidades que pueden regular, solucionar o sancionar violencia en línea



Block together es una iniciativa que tiene como objetivo ayudar a lidiar con el acoso y abuso en Twitter,
permite el bloqueo masivo de usuarios cuando estás siendo agredida o cuando algunas cuentas atacan

a muchas personas de tu comunidad, con la creación de "listas de bloqueos".

Función bloqueo en Twitter, el usuario ya no podrá seguirte, etiquetarte en fotografías o ver tus Tweets.

Las @ respuestas y menciones de las personas bloqueadas tampoco aparecerán en tu pestaña

"Menciones" (Aunque estos Tweets podrían seguir apareciendo en las búsquedas)

1. Lo que entendemos por “violencia en línea” son prácticas muy diversas que a través de la vigilancia, el control o la manipulación de tu información o de tus canales de comunicación tienen como objetivo hacerte daño.

2. No está desconectada de la violencia machista que vivimos en las calles, en las casas y en las camas; es decir, no hay una separación online/offline y es tan real como cualquier otra forma de violencia.

3. En un mismo caso de violencia en línea se pueden manifestar una serie de agresiones distintas. Nombrarlas para reconocerlas y visibilizarlas

4. Por sí mismas, ninguna agresión es más grave que otra y tampoco son necesariamente una escala que va de menor a mayor, aunque en casos sí pueden ser interdependeintes o una habilitar a otra.

Estas violencias causan daño psicológico y emocional, refuerzan los prejuicios, dañan la reputación, causan pérdidas económicas y plantean barreras a la participación en la vida pública y pueden conducir a formas de violencia sexual y otras formas de violencia física.

EFECTOS

Personal en cuanto a las afectaciones físicas y psíquicas que inciden en la vida de la persona
y
Social en cuanto puede provocar que las mujeres se autocensuren y se abstengan de hablar libremente.

Estas situaciones limitan el grado de participación de las mujeres en debates de interés público, proceso de toma de decisiones, y perpetúa la manera en la que se construyen los espacios de ciudadanía digital: en base a la exclusión de las mujeres y otros grupos minoritarios

Impacto físico
Impacto emocional

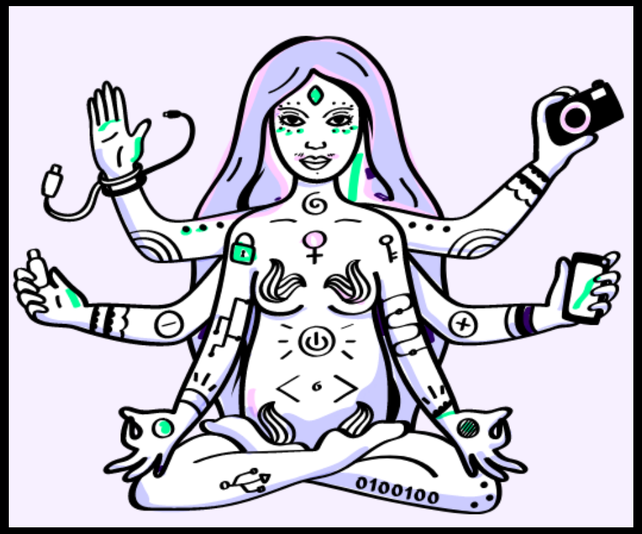
Afectan directamente nuestro derecho de navegar libremente y habitar internet

INTERMEDIARIOS ¿QUÉ SON?

¿QUÉ RESPONSABILIDADES TIENEN LAS PLATAFORMAS?

- Deben adoptar mecanismos de denuncia transparentes para los casos de violencia en línea. Deben ser accesibles, fáciles de usar y de encontrar.
- Deben ofrecer sus Términos de Servicio y plataformas de ayuda en idiomas locales.
- Deben garantizar la seguridad y la privacidad de los datos, y contar con el consentimiento plenamente informado de sus usuarios.
- Deben comprometerse a erradicar la violencia de género en línea, asignando recursos a campañas de información y educación.
- Deben publicar una política clara y amplia sobre cómo moderan los contenidos, para evitar la censura, y poner a disposición procedimientos de revisión y apelación.

Queres saber más...



Conocer para resistir. Hiperderecho
https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf

La violencia digital es real. TEDIC.
https://violenciadigital.tedic.org/

Luchadoras

Ciberseguras
https://ciberseguras.org/tipos-de-violencia-de-genero-on-line-y-autodefensa/Ciber
https://ciberseguras.org/nosotras/

Dominemos la tecnología
https://www.takebackthetech.net/es

Glosario
http://www.libresenlinea.mx/autodefensa/la-violencia-en-linea/glosario-de-ciberataques/

http://papel.revistafibra.info/responsabilidad-intermediarios-internet-analisis-partir-del-caso-maiorana/

http://www.libresenlinea.mx/autodefensa/la-violencia-en-linea/que-responsabilidad-tienen-las-plataformas-de-internet/

https://violenciadigital.tedic.org/#violencia

https://verne.elpais.com/verne/2015/10/05/articulo/1444042741_166153.html

https://violentadasencuarentena.distintaslatitudes.net/una-mirada-latinoamericana/

https://socialtic.org/wp-content/uploads/2017/12/GuiaEstrategias_Ciberseguras.pdf

CUIDADOS DIGITALES #2

¿Qué son los cuidados digitales?

Cuidados digitales: estrategias colectivas de seguridad digital desarrolladas y difundidas por activistas feministas en internet, como una forma de defensa y prevención de los daños producto de los ataques virtuales contra las mujeres y los grupos minoritarios.

Esta manera de abordar las violencias relacionadas con las tecnologías relaciona una larga tradición feminista referida a los «cuidados» como un conjunto de prácticas intrincadas en el patrimonio político-discursivo de la ética feminista, en especial por las contribuciones producidas por los análisis interseccionales y la reivindicación de la hermandad como ética de resistencia.

No existen fórmulas mágicas para lidiar con la violencia,
no hay formas idóneas para vivir una situación así.

SEXTING SEGURO

El sexting es un ejercicio de nuestra sexualidad.

Es un derecho sexual. Es tu cuerpo y es tu derecho. Como en todo acto sexual, existen riesgos, pero eso no significa que no hayan estrategias para hacerlo de manera segura.

El sexting es el envío voluntario de contenido (principalmente fotografías o videos) íntimo y sexual por medio de teléfono móvil, computadora o tableta.

1- Pienso y luego envió

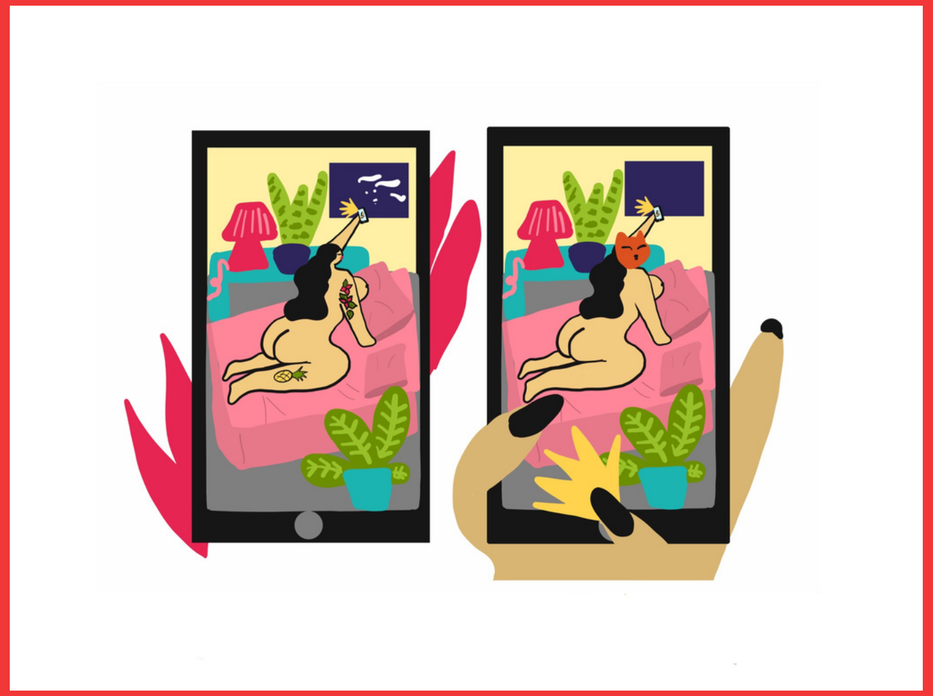
2- Confianza y consentimiento mutuo

3- Elige las aplicaciones

4- Sexting seguro

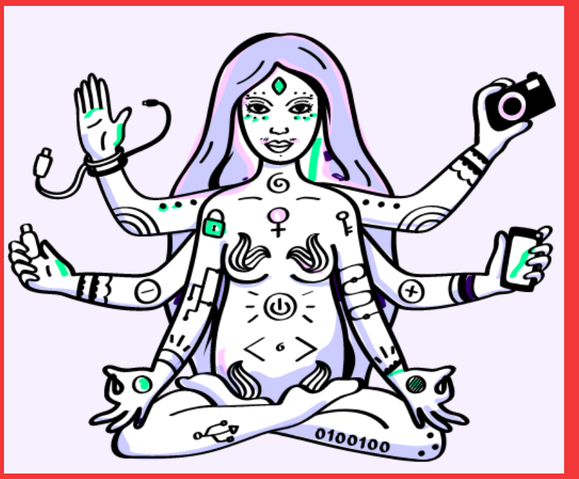
5- Intimidad, creatividad y privacidad

6- Vive la experiencia



DIVIÉRTETE

Queres saber más...



https://socialtic.org/blog/consejos-para-hacer-sexting-seguro/

http://www.libresenlinea.mx/autodefensa/guias-de-reaccion-rapida/tips-para-un-sexting-seguro/

https://www.sextingseguro.com/consejos-sextear-nudes-con-menos-riesgos/

https://luchadoras.mx/mucho-ojo-con-culpar-al-sexting/

https://cyborgfeminista.tedic.org/sexting-sendnudes/

http://www.libresenlinea.mx/autodefensa/internet-feminista/no-es-tu-culpa/

https://hiperderecho.org/sexting/

BÁSICOS DE SEGURIDAD

¿QUÉ ES LA SEGURIDAD DIGITAL?

La seguridad digital: conjunto de hábitos y decisiones que tomamos para mitigar riesgos asociados al uso de la tecnología.

Esta definición no se enfoca en la tecnología, sino en el uso que le damos y las decisiones que tomamos alrededor de esta según nuestro contexto y necesidades.

Aprender sobre seguridad digital implica crear nuevos hábitos, construir nuevos conocimientos y tomar decisiones enfocadas en la privacidad y la seguridad.

Es una invitación a repensar nuestra relación con Internet.

Desde una perspectiva holística, la seguridad digital comprende tres dimensiones:
la seguridad física, la mental y de autocuidados y, por último, la digital.

Apostamos por este enfoque porque implica que aquello que vivimos en Internet también es real y reconoce que los riesgos que vivimos en espacios virtuales fácilmente pueden trasladarse al espacio físico.

Trata tus contraseñas como tu ropa interior

¿Qué nivel de riesgos tengo?

1- contraseñas fuertes

- Nunca envíes tus contraseñas a nadie, bajo ningún concepto.
- Crea contraseñas que no incluyan tu información personal
- Deberían ser largas (de 8 o 10 caracteres hacia adelante)
- Recuerda cambiarlas con cierta periodicidad

Una contraseña se considera segura cuando:

- Es larga (como las frases) y contienen más de 12 caracteres
- Contienen mayúsculas, minúsculas, símbolos y números
- Es privada, ya que no la compartes con nadie
- Es única, ya que no repites la misma contraseñas en varios servicios
- Tiene caducidad

Siempre cierra tu sesión

https://howsecureismypassword.net/

ADMINISTRACIÓN DE CONTRASEÑAS

KEEPASX

HTTPS://KEEPASS.INFO/

MÁS INFORMACIÓN:

HTTPS://SECURITYINABOX.ORG/ES/

TÉRMINOS DE REFERENCIA

Términos de Servicio; No leí: (https://tosdr.org) ofrece una aplicación para obtener resúmenes, en un lenguaje comprensible',' de los Términos de Servicio de muchas plataformas de redes sociales y páginas conocidas.

6 consejos para proteger tu comunicación de ojos intrusos: (https://www.propublica.org/article/six-tips-for-protecting-your-communications-from-prying-eyes)

Básicas para reducir acceso a contenidos y datos

Página web o servicio en linea con información:

asegúrate que este provee una conexión encriptada (el enlace tiene que empezar con https:// y no solo por http, la “s” significa seguro)

Instalar en Firefox, Chrome y Safari, extensiones que mejoran tu privacidad:

Privacy Badger que bloquea rastreadores espías y publicitarios,
Adblock Plus que bloquea ventanas emergentes desagradables
Ghostery que bloquea rastreadores de actores terceros que buscan perfilar tus hábitos en linea.

PUBLICACIÓN DE CONTENIDOS

Cuando compartes detalles personales acerca de tu vida, puedes usar perfiles privados que solo pueden ser accedidos por contactos seleccionados.
Cuando usas plataformas de redes sociales comerciales, tienes que ser consciente de los cambios frecuentes de sus políticas de privacidad.

Cuando escribes o publicas imágenes acerca de eventos públicos, deberías preguntarte si las informaciones que publicas acerca de personas, lugares u otras pueden ponerte o poner alguien a riesgo. Siempre resulta una buena practica pedir primero "permiso" de escribir acerca de personas y eventos, y también establecer acuerdos consensuados acerca de qué y cómo publicar información con todas las presentes a un evento publico.

Puedes oscurecer o volver borrosas las caras en tus fotografías usando una app llamada ObscuraCam (https://guardianproject.info/apps/obscuracam)

Hiperión recomienda:

1. Googleate a ti mismo(a) para ver qué información personal está disponible en Internet, y de ser posible, solicita eliminarla a la persona que administre la cuenta o el sitio en la que esté publicada esta información.

2. Para el caso de redes sociales como Facebook, puedes configurar las opciones d privacidad para que tu perfil no se muestre como resultado de las búsquedas por nombre, número de celular o correo electrónico.

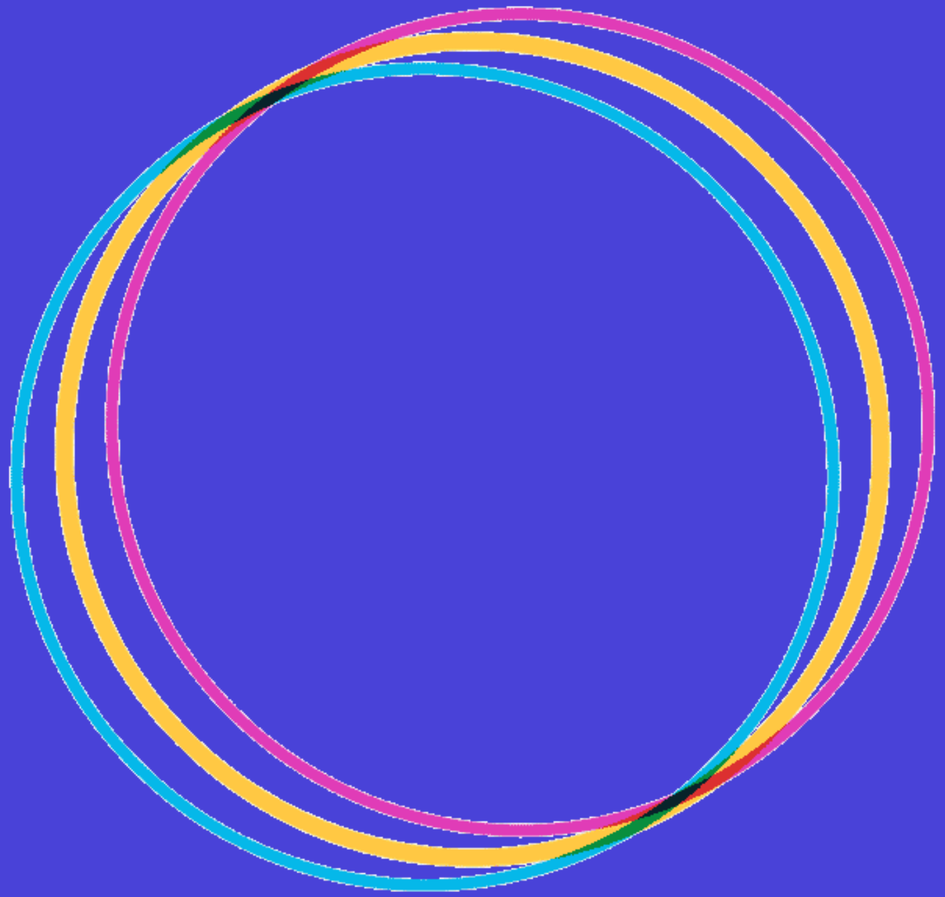
3. De ser necesario, configurar sus redes sociales en privado, deshabilitar la opción de recibir mensajes de personas que no conoces o también filtrar el contenido qu pueden escribir en nuestras publicaciones, videos en vivo, etc. Un ejemplo para Instagram es habilitar el filtro de palabras ofensivas. También está disponible una opción para páginas de Facebook.

4. Limitar el alcance de las personas que pueden ver tu contenido (fotos, publicaciones).

5. Considera crear una cuenta aparte para tus actividades como activista. De ser posible, no compartas - o mantén al mínimo - fotos personales o taggees amistade o familiares. Asimismo, podrías deshabilitar la opción de geolocalización cuando tus posts sean públicos. Toda esta clase de información sobre tu vida personal podría ser usada en tu contra por alguien que busque hacerte daño. Nunca olvides: son tus decisiones y no hay una fórmula única para estar segures.

SEUDÓNIMO

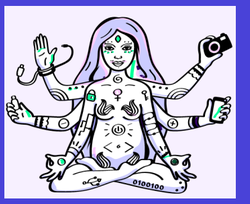
ANONIMATO



IDENTIDAD REAL

IDENTIDAD COLECTIVA

Queres saber más...



¿Cómo la política de Facebook de utilizar el nombre real afecta a personas LGBTQI: (https://www.eff.org/deeplinks/2014/09/facebooks-real-name-policy-can-cause-real-world-harm-lgbtq-community)

La decisión de anonimato para blogueras:(https://advocacy.globalvoicesonline.org/2015/05/01/to-be-or-not-to-be-anonymous-how-should-bloggers-decide/)

Cómo eliminar tu identidad en línea para lograr pleno anonimato en Internet:(http://null-byte.wonderhowto.com/how-to/remove-your-online-identity-ultimate-guide-anonymity-and-security-internet-0131741/)

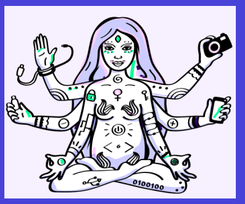
Las muchas razones por las que la gente usa seudónimos: (https://www.eff.org/deeplinks/2011/07/case-pseudonyms)

¿Por qué necesitamos alter egos en línea ahora más que nunca?: (http://www.wired.com/2014/04/why-we-need-online-alter-egos-now-more-than-ever/)

La página web de Guerilla Girls contiene recursos útiles sobre la mujer en el arte (http://www.guerrillagirls.com/info/index.shtml)

https://www.derechosdigitales.org/wp-content/uploads/covid-violencia-domestica.pdf

Queres saber más...



https://www.tedic.org/recomendaciones-de-proteccion-digital-2019/

https://haveibeenpwned.com/

https://www.tedic.org/el-caos-de-las-contrasenas/

https://www.tedic.org/gestor-de-contrasenas-offline/

https://www.tedic.org/el-caos-de-las-contrasenas-preguntas-frecuentes/

https://howsecureismypassword.net/

https://protege.la/guia-de-navegacion-segura-y-anonima/?fbclid=IwAR0vlZVcZCUWq2QDbD1Sq56Bx-0pLfHBowcVQlLbunlqaAYyTIEH3Frs_Us

PROTEGER DISPOSITIVOS

Qué tan seguros son mis dispositivos?

Contar con copias de seguridad de tu info más preciada y guardarla en lugares seguros siempre es buena idea (de paso liberas espacio para más fotitos y videos)

Cifrar archivos

Cifrar tus archivos te sirve para garantizar que el uso o lectura de tu información sea muy difícil de lograr.
Si o si, necesitas de una contraseña para acceder al contenido.
Puedes cifrar todo el contenido de tu disco duro de la computadora con estas opciones (tanto si usas Mac o Windows vas a necesitar una contraseña maestra)

- **Para Windows puedes activar BitLocker en la siguiente ruta:**
- **→ Inicio**
- **→ Panel de control**
- **→ Sistema y seguridad**
- **→ Cifrado de unidad BitLocker**
- **→ Seleccionar cifrado para la unidad (disco duro principia normalmente C:)**

- **Para Mac también es posible activar el cifrado de disco duro en esta ruta:**
- **→ Menú principal (la manzana de la esquina superior izquierda)**
- **→ Preferencias de sistema**
- **→ Privacidad y seguridad**
- **→ Pestaña FileVault**

El phishing es una técnica que busca motivar o engañar a lxs usuarixs para que hagan clic, descarguen o instalen algún programa en su dispositivo (computadora, tablet o celular). Hay distintos tipos de phishing de los cuales debes tomar diversas precauciones.

Recomendaciones:

- Evita descargar archivos de dudosa procedencia
- Evita dar clic en enlaces sospechosos
- Mantén actualizado el sistema operativo de tus equipos
- Usa un antivirus actualizado en tus dispositivos (cel y compu).
- Si notas algún comportamiento extraño no dudes en buscar asesoría.
- En Windows puedes descargar Spybolt para eliminar cierto tipo de malware (programa malicioso), spyware (espía) y adware (publicidad).

Phishing

Verificación en 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.

https://brainstation.io/cybersecurity/two-factor-auth

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 la mayoría 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.

Celular

Bloquear el teléfono con una contraseña, código o patrón
Si alguien quiere acceder a tu celular, sería más complicado si se encuentra bloqueado con una contraseña, pin o patrón que no sea fácil de adivinar (exacto, tu cumple o "12345" no son opción)

Cifrar el teléfono

Para Android, desde la versión 4.0 a la última versión puedes encender encriptar (o cifrar) el dispositivo. Para ello, ve a:
→ Configuración
→ Seguridad
→ Encriptación
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 par de consejos: antes de iniciar el proceso de encriptación, asegúrate que tu teléfono esté de preferencia conectado a la electricidad y tengas copia de seguridad de tus archivos :)

Desactivar la geolocalización

Revisa desde tu configuración, qué aplicaciones tienen acceso a tu ubicación, ya que es posible activar y desactivar esta opción y usarla únicamente cuando la necesites.

Es importante que estos servicios no funcionen como predeterminados pues reduce el riesgo de rastreo de tu ubicación, ahorras batería y reduce el flujo de datos no deseados que inician aplicaciones que se ejecutan de manera secundaria o que tu operador móvil ejecuta de manera remota.

Borrar registro de llamadas

Tu celular todo el tiempo está almacenando una gran cantidad de información. Esta información puede mostrar patrones de conducta de lxs usuarixs. Un buen hábito de higiene digital es borrar cotidianamente el historial de comunicaciones tanto de llamadas como de mensajes que no sean necesarios.

Configura tu privacidad

Tiene que ver con crear reglas sobre quién puede ver tu información y quién no.

Es importante que revises la configuración de privacidad de todas las redes sociales que usas. Algunas vienen configuradas de manera pública y eso significa que cualquiera puede ver la información que publicas.
Al optar por opciones privadas, puedes proteger tu información sensible de personas que te podrían hacer daño.

En Facebook: Visita Configuración > «Privacidad" y asegúrate de que estás de acuerdo con todas las opciones. Te recomendamos la opción «Comprobación rápida de privacidad» en el menú de Ayuda. Además, en la sección de Privacidad, puedes decidir: i) quién puede ver tus contenidos ii) quién puede ponerse en contacto contigo y iii) quién puede buscarte.
En Instagram: Revisa las opciones en Configuración > «Privacidad y Seguridad» para configurar tu cuenta como privada y decidir quiénes pueden enviarte mensajes.
En Twitter: Ve a la sección de configuración y privacidad.
En TikTok: Pulsa Privacidad > Ajustes > Configuración de privacidad y activa la opción 'Cuenta privada'. Allí, tendrás la posibilidad de elegir quién podrá enviarte mensajes, ver tus vídeos, comentar tus publicaciones.

Queres saber más...

https://es.hackblossom.org/cybersecurity/

https://hiperderecho.org/tecnoresistencias/resiste/

https://keepass.info/

https://phishingquiz.withgoogle.com/

https://socialtic.org/blog/tipos-de-phishing-como-identificarlos-y-protegerte/

RETOMANDO EL CONTROL#3

¿Qué podemos hacer frente a una situación de violencia en línea?


acoso.online

DINÁMICA

1- Nos dividimos en grupos

2- Cada grupo va a tener un caso distinto- leerlo en voz alta-

3- Intercambien opiniones.

4- Al final de cada caso hay una serie de preguntas para responder con sus opiniones y según lo que ustedes harían.

PREGUNTAS

- ¿Qué puede hacer la persona que vive esta situación de violencia?
- ¿Qué herramientas tiene la persona que transita por la situación de violencia?
- ¿Existen leyes/normativas que pueden protegerla?, ¿conocen alguna?
- ¿Cuáles son los efectos que esta situación puede tener sobre la persona?
- ¿Cuál es la responsabilidad de quienes poseen y dirigen la plataforma donde ocurrió el incidente?
- ¿Quién más es responsable en este escenario? ¿Cuál es su responsabilidad?
- ¿Cómo podrían responder los movimientos de derechos de las mujeres a esto?

DINÁMICA

Tiempo de intercambio: **45 minutos.**

Las respuestas deben escribirse en pos-it individuales y pegarlas en el papelógrafo.

Pueden haber no respuestas, ya que no sabemos qué hacer o responder, y puede haber más de una respuesta a cada pregunta.

Presentación: **10 minutos**

CASO 1

Eliana (40 años), es activista feminista integrante de un colectivo en Artigas.
Tiene un perfil muy activo en redes sociales(Twitter, instagram, facebook) como activista.
Está en pareja con una reconocida dirigente política del Departamento.

Durante el período que su pareja estaba en campaña en las elecciones departamentales, comenzó a recibir en forma reiterada mensajes agresivos de la cuenta de Twitter @mibuenamor. Por tres meses los mensajes eran insultos y amenazas relacionadas con su identidad sexual y su cuerpo con calificativos tales como: loca, puta, bruja, fea, gorda, lesbiana, tarada y frustrada.
Luego la situación escaló y el perfil agresivo comentaba cada uno de sus posteos sobre eventos y/o actividades

Tras 9 meses de agresiones constantes, Eliana cerró sus cuentas en redes y dejó de militar activamente en la organización feminista a la que pertenece.

CASO 2

Nancy es una deportista afrodescendiente de 30 años que vive en Maldonado.
Es muy reconocida en el país por su actividad.
Nancy tuvo una relación de pareja durante 8 años con Roberto. En diciembre 2020 ambos deciden separarse, ya que la convivencia durante la pandemia fue difícil y se suscitaron varias discusiones fuertes. Desde ese momento cortaron todo vínculo y comunicación.

En marzo de este año, ella comenzó a recibir amenazas por whatsapp de parte de su ex-pareja con publicar fotos y videos íntimos, si ella no accedía a volver con él.

Ante la negativa de Nancy, él publicó las imágenes y videos en facebook y también las envió por messenger a varios de sus contactos.

CASO 3

**Adriana es una adolescente de 14 años. Asiste a un liceo público de Canelones.
Ella se encuentra cursando segundo año en el turno de la mañana.
Debido a la situación sanitaria del país, muchos de los/as docentes comenzaron a crear grupos de Whatsapp para intercambiar con los/as estudiantes tareas y establecer una comunicación más fluida.**

Adriana fue incluida por su profesor de matemáticas dentro de un grupo de Whatsapp. Pocos días después, comienza a recibir mensajes personales de su profesor. Al principio pensó que su profesor quería saber si ella y su familia estaban bien durante la pandemia, y lo mismo haría con otros/otras estudiantes.

Buenas, ¿Cómo estás hoy? ¿Cómo va el encierro? ¿Estás con tu flia?

¿Cómo te despertaste? ¿Estás más linda?

CASO 3

Pero esos mensajes fueron subiendo de tono, ya eran audios invitando a encontrarse.

Buenas! ¿Cómo estás hoy? Nos vemos? Queres tomar un café?

Holaaaa!!! no me contestassss. Si quieres nos podemos ahorrar los besos y vamos directo a la cama!!!

empezamos con el pie izquierdo te propongo algo...
Te pasas por mi casa!!!

Buenas!!! ¿Sabes lo que me gusta de las chicas como vos? Foto de su miembro

Ella decide no responder, como una táctica para desactivar la situación. Ante la no respuesta empezó a recibir fotos de los genitales del profesor.

CASO 4

Daniela es una mujer trans de 33 años.
Con dos de sus amigas más cercanas, Mariana y Sol, crearon una organización para promover la igualdad de las personas LGBTQI+ en Montevideo.
Debido a su rol en la organización, las han invitado a eventos en torno a los derechos LGBTQI + y han asistido a manifestaciones para apoyar su defensa.
Daniela ha dado notas en la prensa, hablando en contra de la masculinidad tóxica y en defensa de los derechos LGBTQI+.
Hace seis meses, Daniela, Mariana y Sol comenzaron a recibir mensajes en sus cuentas personales de Facebook. Estos mensajes provienen de una cuenta denominada Anonymus y envia mensajes que fomentan un discurso sistemático de intolerancia y discriminación, contra su organización y contra de personas LGTBIQI+.

A su vez, de esta cuenta se solicitaba que denuncien sus posteos, cuentas personales y de la organización.

CASO 4

Estos malditos desviados, son la causa de los problemas de los jóvenes. denuncien sus posteos.

No permitan que sean un mal ejemplo para los jóvenes de bien, denuncien sus posteos por incitar a vivir contra las reglas de la naturaleza.

Lo que no soportamos es que se metan en nuestras casas, nos digan cómo tenemos que vivir y educar a nuestros hijos. Que orgullo ser hombre. tenemos que ir por ellos, denuncien sus posteos!

Finalmente, deciden bloquear la cuenta y no responder. Pero, siguen apareciendo más mensajes de diferentes usuarios/as en sus cuentas personales de Facebook, twitters y en las redes de la organización.

CASO 4

Los mensajes se vuelven progresivamente más agresivos y comienzan a recibir más solicitudes de contactos en ambas plataformas.

Un hombre no puede quedar embarazado. Un hombre no tiene útero ni óvulos.

Lo próximo nos instalan un chip de arcoiris a todos y nos volvemos todos homosexuales...!!!!

Por lo tanto, deciden bloquear a esos usuarios e intentan ignorarlos.

La cuenta del perfil anonymous y varios seguidores comenzaron a reportar sus posteos como abusivos en Twitter. La cuenta de Twitter de su organización fue suspendida.

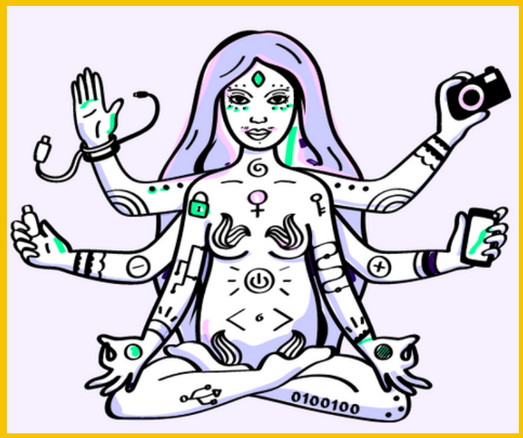
CASO 5

Beatriz vivió un hackeo de varias de sus cuentas en redes sociales: instagram, facebook, twitter y gmail por parte de una expareja.

Esta situación le impide el acceso a las mismas y comienza a recibir mensajes a su celular donde le pide rescate.

Beatriz no accedió a pagar el rescate, pero días después un de los supervisores de su trabajo le avisa que a la cuenta de Twitter de la empresa llegaron varios msjs con fotos con la cara de ella y un link a un sitio de pornografía.

Queres saber más...



https://seguridad-digital.org/por-que-y-como-registrar-y-documentar-incidentes/

https://sursiendo.org/2020/10/imagenes-herramienta-de-registro-de-incidentes-digitales/

DISCURSO ANTI-DERECHOS EN INTERNET

¿Qué es el discurso de odio? ¿Cómo identificar tácticas anti-derechos en internet?

Ilustración: Candy Rodríguez

¿Qué es y qué NO es libertad de expresión?

- **Es proteger la diversidad de discursos, la disidencia, la manifestación de estilos de vida variados, a manifestarnos y ser quienes y cómo somos.**

- **Implica proteger cierto tipo de discurso aunque pueda ofender.**
  - **Son expresiones protegidas: crítica, desacuerdo, disidencia, parodia.**
  - **No son expresiones protegidas: fomento del odio sistemático hacia grupos sociales, manipulación de información con el objetivo de perjudicar, exposición no consentida de imágenes íntimas, amenazas.**

¿QUÉ ES EL DISCURSO DE ODIO?

- **Concepto muy amplio: no existe una definición única y universalmente aceptada.**
- **Se pueden clasificar distintos tipos según su gravedad y consecuencias.**
- **Algunos tipos son delito y los Estados (de acuerdo con el derecho internacional de los derechos humanos) deben tomar medidas para restringir o incluso prohibir estos discursos.**
- **Sin embargo, no todos los discursos ofensivos se deben restringir.**
- **La prohibición puede ser contraproducente si no se atacan las raíces sociales del discurso de odio.**

Libertad de expresión y discurso de odio: ¿y entonces, qué hacemos?

- **La protección de la libertad de expresión y la lucha contra la violencia línea no son opuestas, se complementan.**

- **La lucha no debe basarse en el control de las comunicaciones para la vigilancia y la censura.**

- **La vigilancia y la censura perjudican la presencia del contra-discurso feminista frente a la narrativa anti-derechos en internet.**

¿Cómo se manifiesta la narrativa anti-derechos en internet?

- **"Para que los espacios virtuales se vuelvan espacios irrespirables existen esfuerzos sistemáticos y coordinados ... La política e internet deben ser, para esta agenda, espacios invivibles y sofocantes para mujeres y no binaries". (Florencia Goldsman).**
- **¿Quiénes? Estados (violencia institucional) y otros agentes hegemónicos, con tácticas de acoso político dirigido.**
- **¿Cómo nos afecta?**
  - **Individualmente: desde auto-censura al abandono de los espacios online.**
  - **Colectivamente: Internet se vuelve un espacio minado donde nuestras disputas se minimizan y marginan.**
  - **Culturalmente: función disciplinadora y normativizante.**

6 TÁCTICAS PARA LLENAR INTERNET DE

- **REGLA 1: Convencer a los demás de que las mujeres (y disisencias) son maliciosas: no son aptas para la política.**
- **REGLA 2: Denunciar a las mujeres como demasiado estúpidas para la vida pública.**
- **REGLA 3: Hacer que las mujeres tengan miedo de responder.**
- **REGLA 4: Elogiar a las mujeres por ser sexys y condenarlas por ser sexuales.**
- **REGLA 5: Mostrar a las audiencias que, como en los cuentos de hadas, los hombres fuertes van a salvarnos.**
- **REGLA 6: Demonizar los valores que las mujeres sostienen.**

Fuente: https://genderit.org/es/feminist-talk/internet-minada-y-seis-reglas-para-entender-las-narrativas-anti-derechos

ESTRATEGIAS (1): HUMOR, CREATIVIDAD Y CONTRADISCURSO

https://mtroll.karisma.org.co

ESTRATEGIAS (2): RESISTENCIA / RESILIENCIA

https://acoso.online/uy

https://vita-activa.org/

ESTRATEGIAS (3): VISIBILIZAR, SENSIBILIZAR Y PONER EN DISCUSIÓN PÚBLICA

https://violenciadigital.tedic.org/

COLLAGE COLECTIVO

Hackeo ciberfeminista de discursos anti-derechos


TE DIC·
TECNOLOGÍA & COMUNIDAD
CIBORRGANIZADAS
NOS QUEREMOS
NO +
transfeminicidios
ME ENTERRARON
ME ENTERRARON

De qué se trata

- **Contar nuestra propia historia como un acto radical.**
- **Remixar diversas narrativas personales del encuentro.**
- **Crear y preservar memorias.**
- **Documentar aprendizajes: qué me gustó y qué no, qué información quiero guardar para más adelante, qué más quiero saber/aprender, qué puntos son importantes para compartir con mis compañeres, apuntes, reflexiones críticas.**

Materiales

- **Hojas para recortar impresas**
- **Diarios y revistas**
- **Papeles de colores**
- **Tijeras**
- **Pegamento**
- **Marcadores, lapiceras, lápices de colores**
- **Material personal: fotos de sus lugares y espacios, alguna selfie impresa, fotocopias de páginas de sus libros favoritos, recortes de revistas con imágenes que les gusten, etc.**

Tips básicos de collage

- **Inspirate con las imágenes: el collage se trata de partir de las imágenes que tenés enfrente, antes que partir de un tema.**
- **¡No uses todas las imágenes que te gustan! El collage empieza con una selección.**
- **Una "fórmula" simple para empezar: elegí un fondo (paisaje, textura, etc.) imágenes repetidas (círculos, zapatos, etc.) y una imagen central (un pájaro).**
- **Mezclá universos: botánico y cyber, animal y humano, retro y futurista, etc.**
- **Usá formas geométricas y texturas, o crealas.**
- **Intervení las imágenes, modificalas.**
- **Seleccioná uno o dos colores que se repitan.**
- **Armá una composición con cierta armonía, pero siempre un poco inusual.**
- **CORTAR: con tijera o rasgando, por el contorno o dejando bordes.**
- **PEGAR: podés armar una composición y después pegar, o ir pegando imágenes a medida que trabajás en el collage.**
- **Si estás indecisa sobre cómo seguir, no mires tu collage por un rato, dejalo y volvé después.**
- **Sumá tu collage al collage colectivo, o intervenilo directamente con más imágenes.**

¡Descargá y reutilizá esta presentación!
Disponible en:
https://share2.apc.org/s/xi5JGGgYJ8zdZ5P