Taller Autodefensa Digital ante el Ciberacoso a través de Fanzines

Duración: Tres sesiones presenciales de 90 minutos + acompañamiento semanal

Presentación del Taller

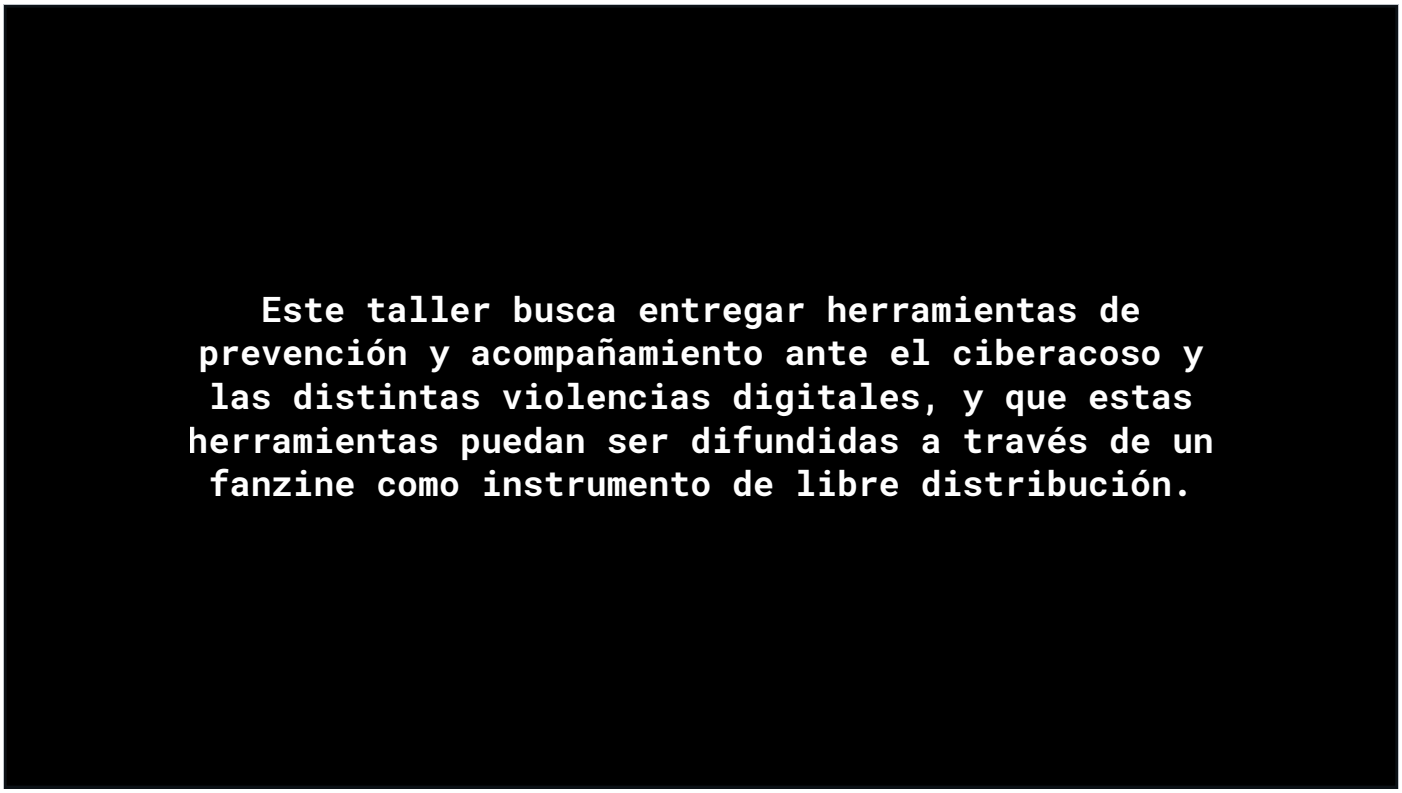
Presentación de quien facilita el taller.

MÓDULO 1 : CIBERACOSO Y AUTODEFENSA DIGITAL

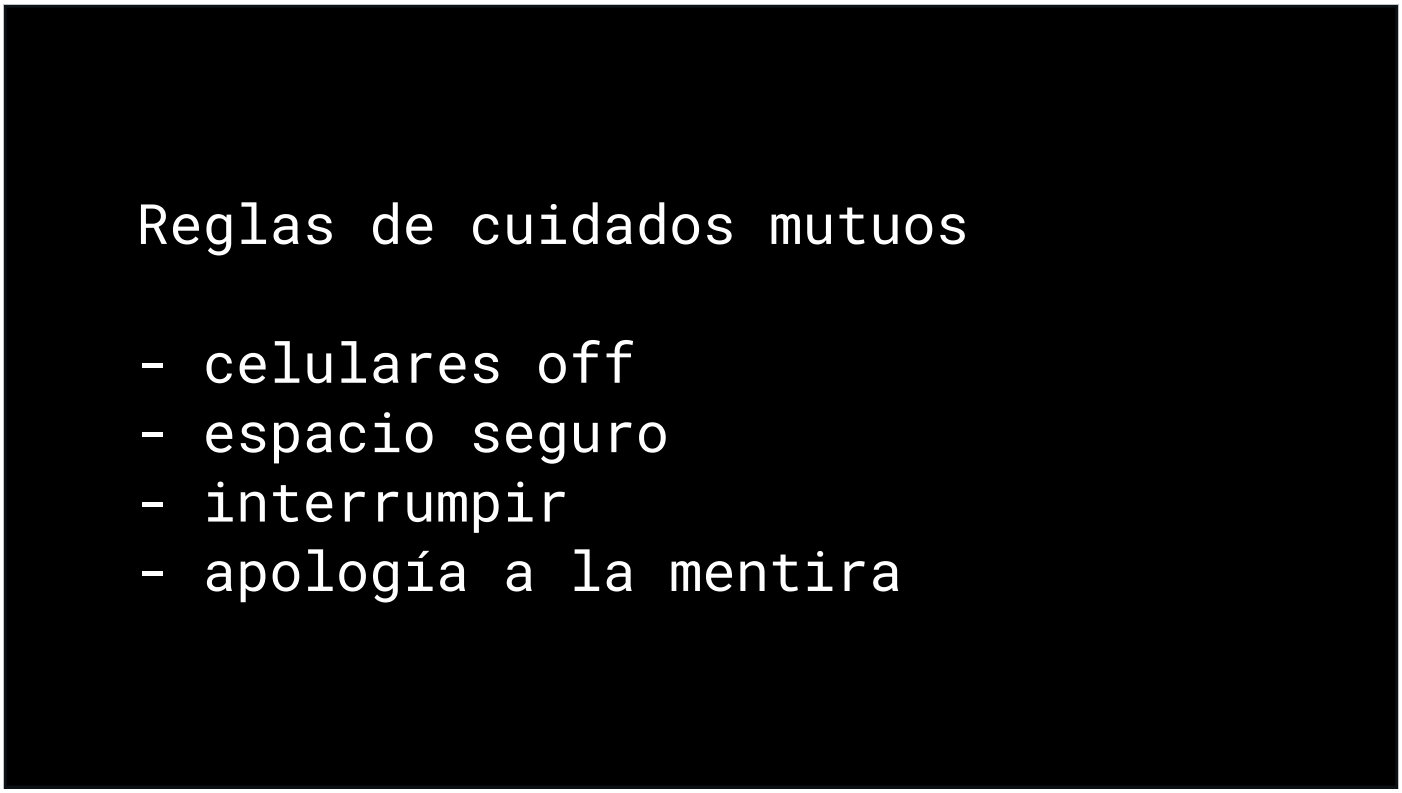
Clase teórica e informativa sobre el fenómeno del ciberacoso y las formas de autodefensa digital.

Presentación modulo 1 y forma de trabajo

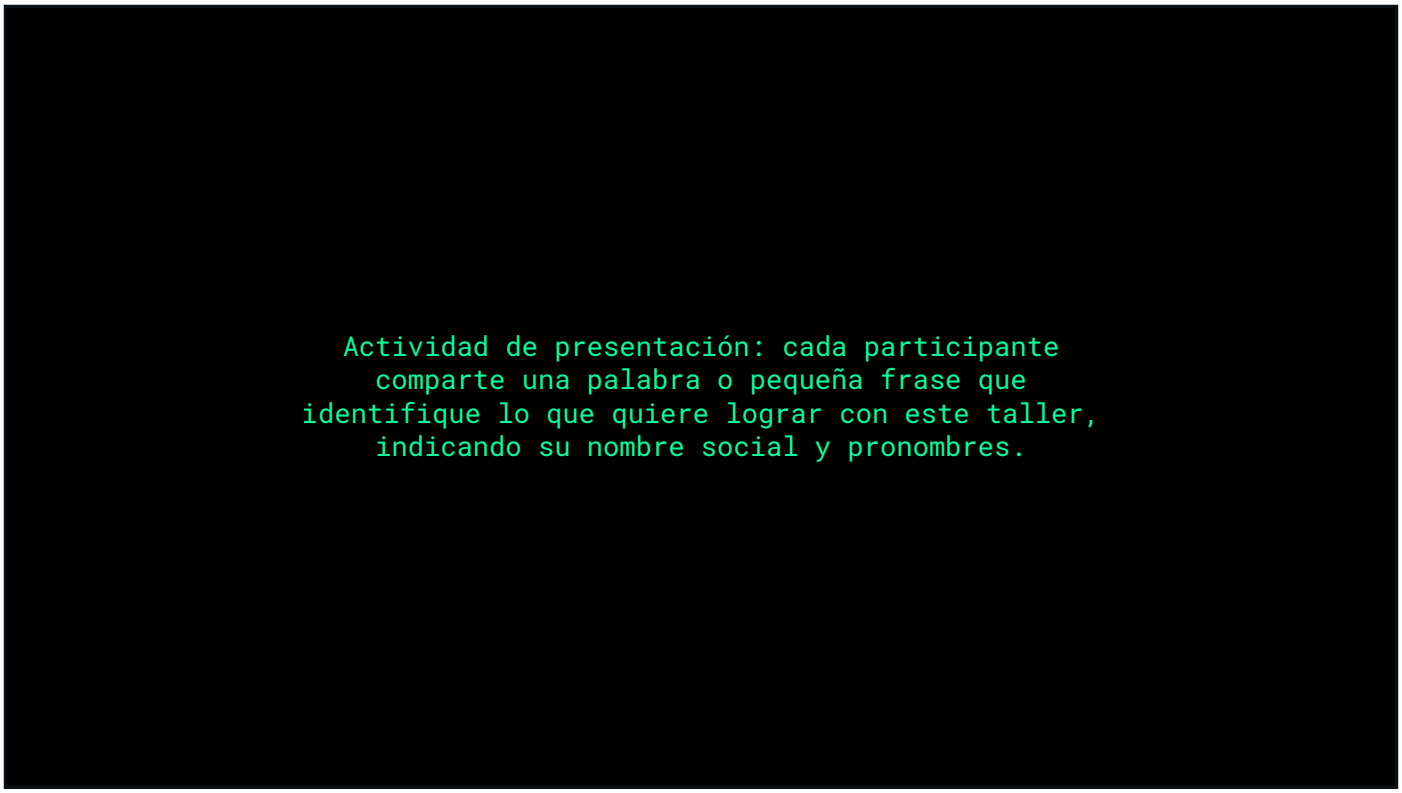
(explicar lo del acompañamiento entre semana)



Objetivo del taller.

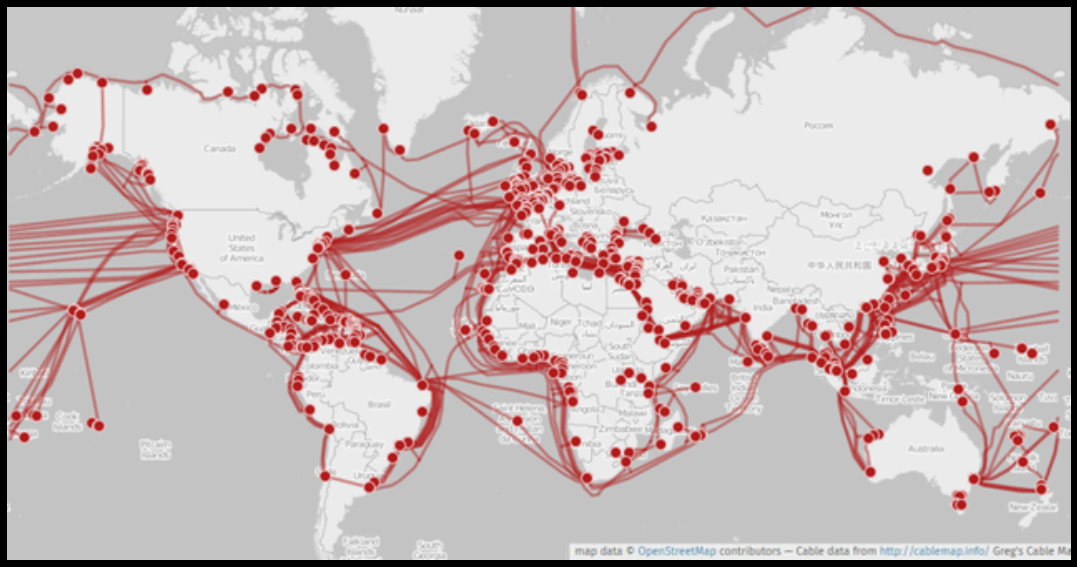


Explicar las reglas de cuidados mutuos durante el taller.



Actividad de presentación

Antes de hablar sobre CiberAcoso



Antes de hablar sobre CiberAcoso.

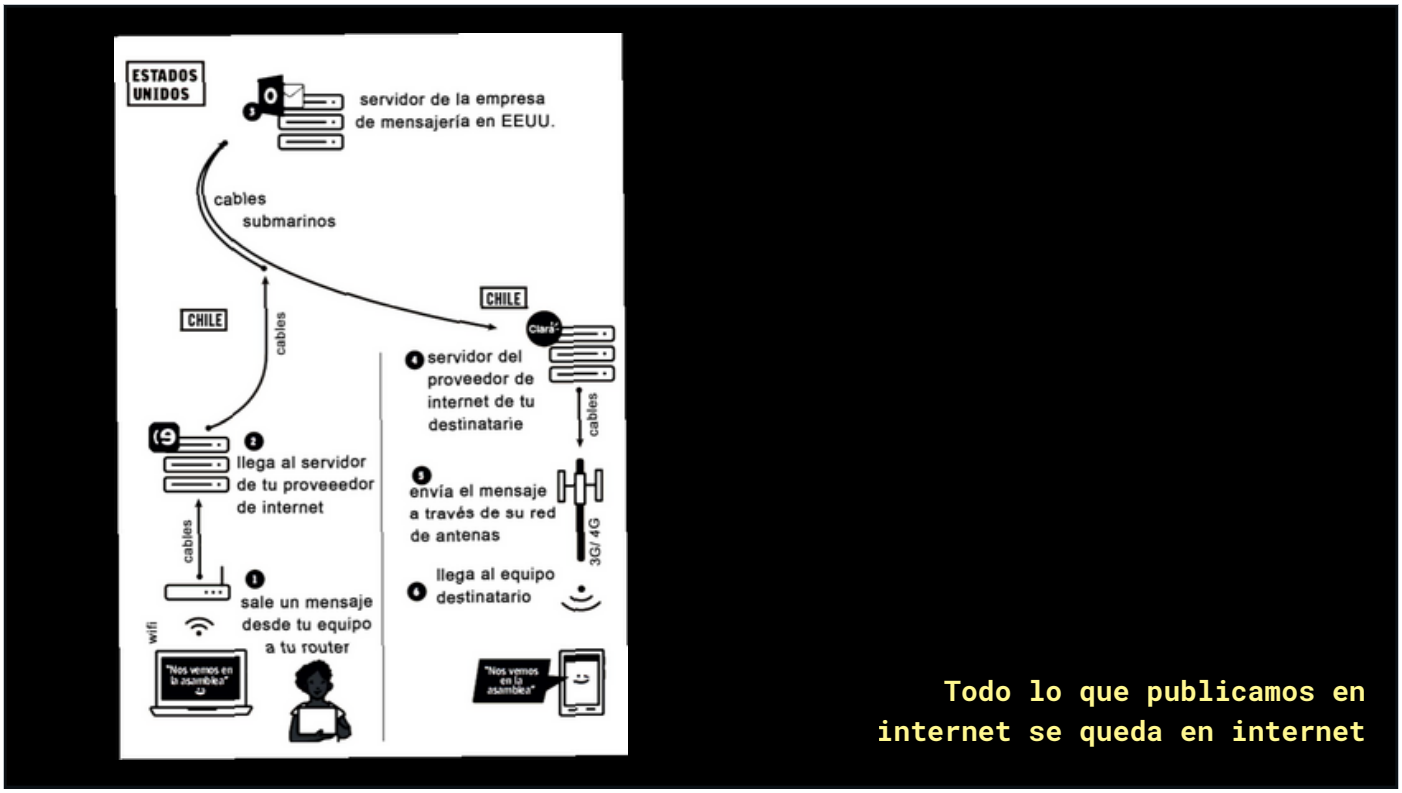
¿Qué es el internet?

El internet es una red mundial de computadoras y dispositivos conectados que permite intercambiar información, comunicarnos y compartir contenido.

Es infraestructura global formada por servidores, cables, satélites y redes inalámbricas que conectan millones de equipos.

Pero más allá de lo técnico, internet también es un espacio social y político:

Ejemplo para explicar en clase:
“Internet no es solo ‘la nube’ o las redes sociales; es una gran red donde cada acción deja una huella. Es como caminar por la arena: todo lo que hacemos deja marcas, aunque luego no las veamos.”



¿Qué quiere decir que todo lo que publicamos en internet se queda en internet?

Significa que toda información que compartimos —fotos, textos, audios, videos, ubicaciones— deja una copia o registro en algún lugar de esa red global, incluso si después la borramos.

Esto ocurre porque:

- Los servidores donde se guarda la información pueden mantener copias.
- Otras personas pueden descargar, reenviar o hacer capturas.
- Los algoritmos y sistemas de inteligencia artificial también recopilan y almacenan datos para analizar nuestro comportamiento.

Ejemplo simple:
Si publicas una foto y la borras al minuto, esa imagen puede haber sido vista, descargada o guardada por alguien más, o quedar almacenada en el servidor de la plataforma.
Por eso se dice que “todo lo que subimos a internet deja huella digital”: aunque no siempre sea visible, sigue existiendo en alguna parte.

TIPOS DE VIOLENCIA EN INTERNET

- Spam
- Stalking
- Troleo
- Sextorsion
- Grooming
- Ciberacoso
- Phishing
- Doxing
- Robo de identidad

Tipos de violencia en internet

Spam

Es el envío masivo de mensajes no deseados o irrelevantes, generalmente con fines publicitarios o engañosos.
Satura correos, redes o comentarios, y puede ocultar intentos de estafa o enlaces peligrosos .
Ejemplo: correos que ofrecen premios falsos o mensajes automáticos con enlaces sospechos os.

Stalking (ciberacecho o acecho digital)
Consiste en vigilar, seguir o monitorear constantemente a una persona a través de redes sociales, correos o GPS, sin su consentimiento.
Suele ser una forma de control y acoso psicológico, especialmente en contextos de pareja o exparejas.
Ejemplo: revisar todas tus publicaciones, rastrear tus ubicaciones, crear cuentas falsas para observarte.

Troleo (Trolling)
Acciones destinadas a provocar, humillar o generar conflicto en espacios digitales, generalmente mediante comentarios ofensivos o burlas.
A menudo se justifica como “humor” o “libertad de expresión”, pero puede ser una forma de

violencia psicológica sostenida.
Ejemplo: comentar agresivamente en publicaciones feministas o de disidencias para desestabilizar o ridiculizar.

Sextorsión (extorsión sexual digital)
Forma de chantaje o amenaza digital donde alguien intenta obtener dinero, favores o silencio a cambio de no publicar imágenes íntimas o información personal.
A menudo se origina en relaciones de confianza o engaños en línea.
Ejemplo: alguien amenaza con difundir tus fotos privadas si no envías más contenido o diner o.

Grooming
Práctica en la que una persona adulta se gana la confianza de un menor o persona vulnerable con el fin de obtener contenido sexual o establecer contacto físico.
Se realiza a través de redes, juegos en línea o mensajería.
Ejemplo: un adulto finge ser adolescente para acercarse a una menor y pedirle fotos íntimas.

Ciberacoso
Uso intencional y repetido de medios digitales para hostigar, intimidar, humillar o amenazar a una persona o grupo.
Puede manifestarse en insultos, difusión de rumores, manipulación de imágenes, o ataques coordinados.
Ejemplo: mensajes ofensivos diarios o campañas para desacreditar tu trabajo artístico o acti vismo.

Phishing
Técnica de engaño digital para obtener contraseñas, datos bancarios o personales, haciéndose pasar por una institución o persona de confianza.
Ejemplo: recibir un correo que simula ser de tu banco y te pide “verificar tu cuenta” mediante un enlace falso.

Doxing (o Doxxing)
Publicar o difundir información personal o privada (nombre legal, dirección, teléfono, datos familiares) sin consentimiento, con el fin de intimidar o dañar.
Es una forma grave de violencia digital, usada para exponer y amenazar activistas, periodistas o mujeres visibles en redes.
Ejemplo: compartir en grupos tus datos personales o fotos familiares tras una discusión en lí nea.

Robo de identidad
Cuando alguien usa tu nombre, fotos, datos o cuentas para hacerse pasar por ti y cometer

fraudes, acosar o dañar tu reputación.
Ejemplo: crear un perfil con tu foto para contactar a tus amistades o seguidores y pedir dinero.

¿Qué es el ciberacoso?

Se define como un comportamiento intencional y repetido que usa dispositivos electrónicos o medios digitales para dañar, amenazar o avergonzar a otra persona.

Según Cibermujeres, el ciberacoso es una forma de violencia en línea contra las mujeres que busca intimidar, controlar o silenciar.

Que es el ciber acoso

Se define como un comportamiento intencional y repetido que usa dispositivos electrónicos o medios digitales para dañar, amenazar o avergonzar a otra persona. Definición de Cyberbullying Research Center.

Según Cibermujeres, el ciberacoso es una forma de violencia en línea contra las mujeres que busca intimidar, controlar o silenciar.
Puede manifestarse como amenazas, difusión de información personal, manipulación de imágenes, troleo coordinado o exclusión digital.

En los entornos digitales, las mujeres y disidencias enfrentan ataques específicos de género, relacionados con estereotipos, roles y sexualización.

El patriarcado tambien esta en el espacio virtual .

Impactos Documentados

Ansiedad, depresión, alteración del sueño, disminución del bienestar, incluso ideación suicida en contextos juveniles.

El ciberacoso puede tener profundos efectos biopsicosociales en sus víctimas.

Impactos documentados Se adjunta estudio en ingles. Disponible en la Bibliografía https://ciberacoso.neocities.org/

Cómo operan las redes sociales privativas y la inteligencia artificial en reproducir el ciberacoso

- La redes privativas:
- Recolectan datos de forma centralizada.
- Los algoritmos no están diseñados para diferenciar contenidos.
- El algoritmo solo amplifica lo que considera de interés ante el uso.
- Suelen amplificar el contenido violento por su atractivo emocional.
- Los algoritmos tienen sesgos de genero y racismo.

- Inteligencia Artificial:
- Con las imágenes generativas se ha abierto una nueva forma de violencia digital al crear imágenes sin consentimiento de las partes.

Como operan las redes sociales privativas y la inteligencia artificial en reproducir el ciberacoso

Las plataformas privativas (centralizadas, de propiedad corporativa) suelen recolectar datos, generar perfiles de usuario, alimentar algoritmos de visibilidad que pueden amplificar contenidos agresivos o de acoso.

Estudios recientes muestran que sistemas de IA pueden detectar comportamientos de ciberacoso, aunque hay retos de privacidad cuando se monitorean plataformas cifradas o privadas.

En contraste, plataformas federadas o del Fediverso (como Mastodon) representan una estructura más descentralizada, donde los usuarios y comunidades tienen mayor control sobre normas, moderación, datos personales.
Los algoritmos tienden a reproducir sesgos de género y racismo, haciendo más visibles los ataques contra mujeres o disidencias.

Cibermujeres propone un enfoque de autonomía digital: comprender cómo funcionan estas plataformas es el primer paso para elegir espacios más éticos y comunitarios.
Documento disponible en la bibliografía en https://ciberacoso.neocities.org/

El Fediverso (Mastodon, Pixelfed, PeerTube) ofrece alternativas descentralizadas donde cada comunidad define sus reglas y su cultura de cuidado.

PRÁCTICAS TÉCNICAS DE AUTOCUIDADO DIGITAL

Prácticas recomendadas:

- Usar contraseñas seguras y únicas.
- Habilitar autenticación en dos pasos.
- Actualizar software con regularidad.
- Revisar la configuración de privacidad.
- Limitar permisos de cámara, micrófono y ubicación.
- Hacer copias de seguridad cifradas.
- Cuidar la energía: pausas, descanso, desconexión.

El autocuidado digital no es individualismo; es una forma de resistencia y defensa del derecho a existir en línea sin miedo.

- Prácticas recomendadas:
- Usar contraseñas seguras y únicas (preferir administradores locales).
- Habilitar autenticación en dos pasos.
- Actualizar software con regularidad.
- Revisar la configuración de privacidad.
- Limitar permisos de cámara, micrófono y ubicación.
- Hacer copias de seguridad cifradas.
- Cuidar la energía: pausas, descanso, desconexión consciente.

PRÁCTICAS TÉCNICAS DE AUTOCUIDADO DIGITAL

Ejercicio Mi Identidad en Internet:

- Googleate.
- Cual es mi huella en internet.
- Autoevaluación, lo que esta en internet sobre mi me gusta?

Ejercicio de autogooglearse usando Nombre y Apellidos legal completo.

PRÁCTICAS TÉCNICAS DE AUTOCUIDADO DIGITAL

1) Cuestionar antes de compartir.

2) Autostalkeo y verificación de interlocutores.

3) Revisar configuración de seguridad y privacidad en las cuentas. Siempre.

Reflexión sobre la autoformación.

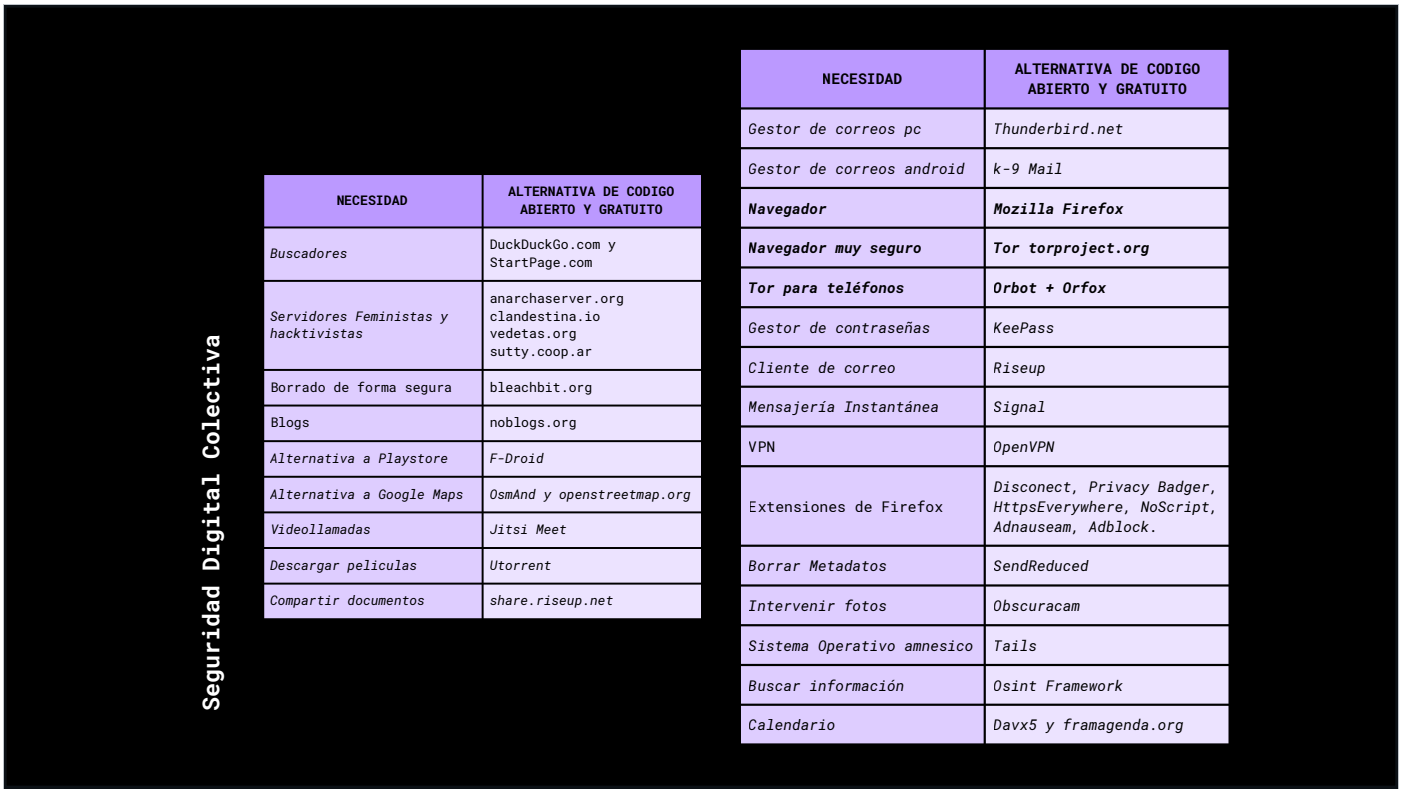
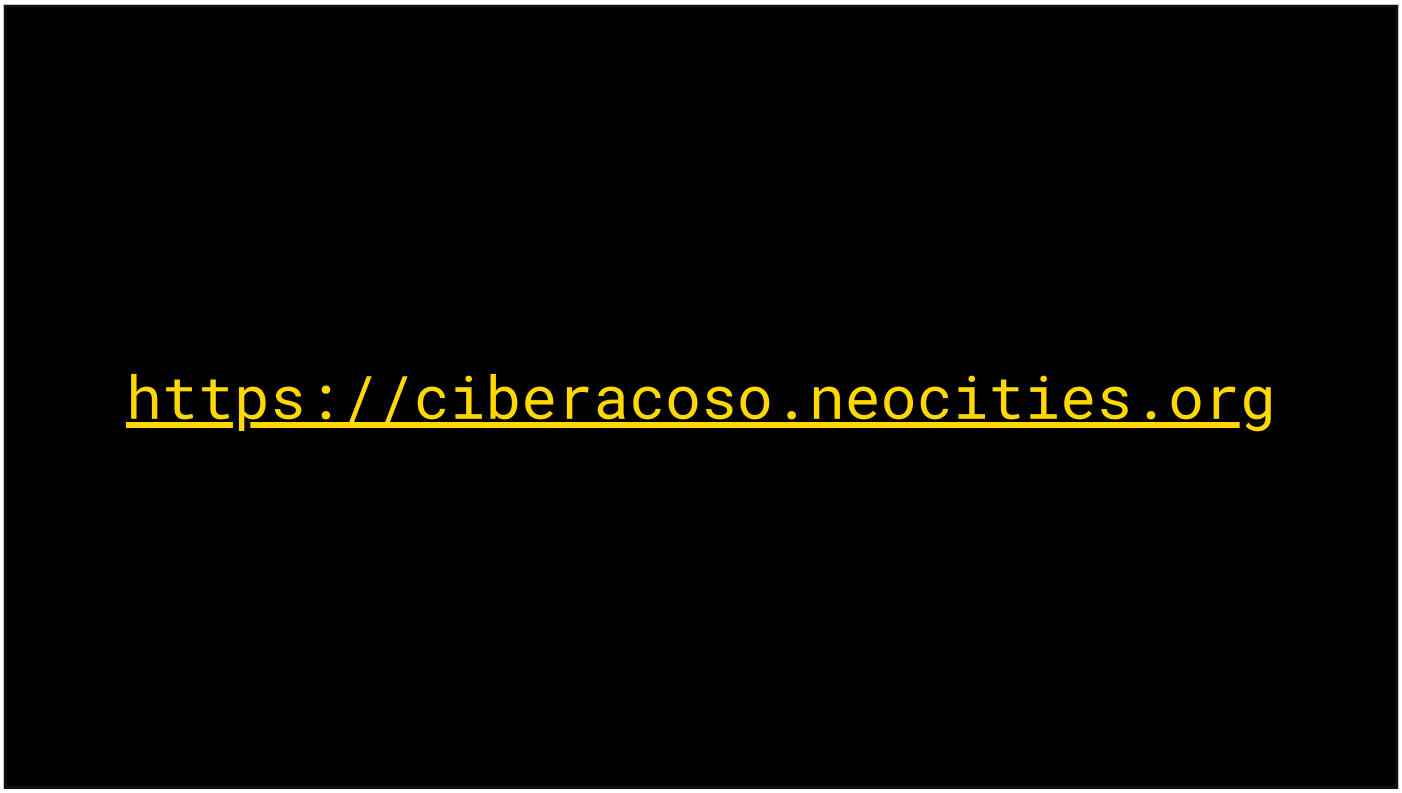


Tabla con alternativas de sofware libre, tabla actualizada en https://ciberacoso.neocities.org/

Revisar listado más actualizado en https://ciberacoso.neocities.org/

CÓMO ACTUAR ANTE UN ATAQUE

- Documentar: capturas de pantalla, URLs, hora, fecha.
- Bloquear y reportar al agresor/a o contenido.
- No interactuar directamente con la cuenta agresora.
- Proteger datos personales (revisar contraseñas, visibilidad).
- Buscar contención emocional y comunitaria.
- Solicitar apoyo técnico o legal si el caso escala.
- Denunciar colectivamente: registrar incidentes para construir estadísticas y memoria.



https://ciberacoso.neocities.org/

Este sitio web es el repositorio donde pueden encontrar toda la bibliografía, material extra y links de interes para investigar más sobre CiberSeguridad, Autonomía digital, Fediverso y Fanzines.