



CIBERMUJERES



Privacidad

Privacidad

**INSTITUTE FOR
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



Esta obra se encuentra licenciada bajo Creative Commons
Atribución-CompartirIgual 4.0 Internacional (CC BY-SA 4.0).

<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

Índice general

1 Privacidad	5
Conducir la sesión	6
Parte 1 – ¿Realmente tenemos privacidad?	6
Parte 2 – “Auto-doxeo”	7
Parte 3 – ¿Y ahora qué hacemos?	8
Referencias	9

Privacidad

- **Objetivos:** Introducir el concepto de privacidad e identificar información sobre nosotras mismas que está en internet.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
 - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
 - Nuestros derechos, nuestra tecnología¹
 - ¡Pregúntame cualquier cosa!²
 - Apps & Plataformas online: ¿Amigo/a o enemigo/a?³
 - Multitudes interconectadas⁴
 - Hagamos doxxing al troll⁵
- **Materiales requeridos:**

¹<https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/nuestros-derechos-nuestra-tecnología/>

²<https://cyber-women.com/es/privacidad/pregúntame-cualquier-cosa/>

³<https://cyber-women.com/es/privacidad/apps-y-plataformas-online/>

⁴<https://cyber-women.com/es/privacidad/multitudes-interconectadas/>

⁵<https://cyber-women.com/es/violencia-en-línea-contras-las-mujeres/hagamos-doxxing-al-troll/>

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- **Recomendaciones:** Algunas participantes pueden sentirse incómodas o disgustadas con la información pública que encuentren sobre ellas mismas en internet en el ejercicio de “auto-doxeo” de esta sesión. si esto ocurre, asegúrate de dedicar suficiente tiempo al final de la sesión para crear estrategias de respuesta. las participantes deben tener acceso a un dispositivo con conexión a internet para la parte práctica de la sesión.

Esta sesión incluye información de la sección “Auto-doxeo y recuperar el control” del manual “Zen y el arte de que la tecnología trabaje para ti” del colectivo Tactical Tech.

Conducir la sesión

Parte 1 – ¿Realmente tenemos privacidad?

1. Inicia la conversación preguntándole al grupo si creen que existe la privacidad real. Después pregúntales qué es la privacidad para ellas. Comparte tu perspectiva a modo de ejemplo. Subraya que la intención del ejercicio es que vayan reclamando su derecho a la privacidad.
2. Pídeles compartir algunos ejemplos de factores que podrían estar interfiriendo en el control que tienen sobre sus datos, información personal y otros elementos. Podrían estar relacionados con prácticas personales, las plataformas a las que confían su información, el conocimiento que tienen sobre las herramientas y dispositivos que utilizan o las acciones de los demás en sus redes.

Parte 2 – “Auto-doxeo”

3. Explica a las participantes qué significa “Doxxing”: en pocas palabras, es la práctica de obtener una gran cantidad de información personal sobre alguien y hacerla pública (generalmente en línea). Puntualiza que a veces el doxxing se utiliza contra personas como táctica de venganza y, generalmente, se emplea para poner en peligro, acosar o amenazar a activistas y defensoras.
4. En esta parte de la sesión, practicarán el “auto-doxeo” como una manera de averiguar cuánto (y qué tipo de) información podemos encontrar sobre nosotras mismas online. Aclara que es un método preventivo a la hora de reducir la cantidad disponible de información (siempre que sea posible).
5. Las participantes abren un documento de texto en blanco en sus computadoras o anotan en un trozo de papel. También inician su navegador web - utilicen un navegador distinto al que acostumbran utilizar- para que no inicie sesión automáticamente en sus cuentas.
6. Antes de comenzar a navegar, cada participante crea una lista de todas sus cuentas públicas y perfiles en plataformas de redes sociales; después, anota palabras clave o frases que pueden estar asociadas a ellas, incluyendo información como:
 - La ciudad donde nacieron
 - La ciudad donde viven
 - Su dirección postal
 - La organización en la que trabajan (o con las que colaboran regularmente)
 - Sus áreas de acción en sus activismos
 - Proyectos y campañas principales en las que participan/trabajan
7. Para empezar su auto-doxeo, primero deberán buscar sus cuentas y perfiles online (deberían poder ver estas cuentas/perfiles como aparecerían para el público general ya que no están con sesión iniciada en sus cuentas) y tomar nota de qué información encuentran sobre si mis-

mas.

8. A continuación, buscan sus nombres y otras palabras clave de la lista que crearon antes, utilizando el buscador de Google, DuckDuckGo, Facebook, Twitter y otras plataformas. Recomendamos algunas cuestiones más para este paso:
 - Para Google y DuckDuckGo, pueden hacer búsquedas de imágenes y vídeos, aparte de búsquedas de texto.
 - Si conocen determinadas bases de datos online - para ciudades, gobiernos, etc. - donde podrían aparecer sus datos, pueden realizar estas búsquedas ahí también.
 - Si tienen un sitio web propio, pueden buscar la url en <https://whois-search.com> para averiguar qué información aparece sobre ellas en el registro público de dominios.

Parte 3 – ¿Y ahora qué hacemos?

9. Explica al grupo que, a través de su auto-doxeo, quizás encuentren información sobre ellas que no sabían que estaba disponible públicamente, incluyendo cuentas que ya no utilizan y ni se acordaban que tenían.
10. Pídeles que revisen sus anotaciones y piensen qué pasos podrían seguir para tomar más control sobre lo que otras personas pueden encontrar sobre ellas en internet. Pueden realizar una lista de tareas de estos pasos que puede incluir acciones como cerrar determinadas cuentas, editar su información y/o configuraciones de privacidad de sus cuentas de plataformas de redes sociales, activar la opción de registro privado de dominio en su hosting de dominio, etc.
11. Conforme vayan haciendo estas listas de tareas, comparte algunos recursos útiles para ayudarlas a implementar algunos de estos pasos.

Herramienta de bloqueo temporal de URL: Sirve para bloquear resultados de búsquedas de sitios. No elimina el contenido, pero bloquea, hasta que se actualicen en los sitio(s) fuente, resultados de búsqueda de contenido antiguos que pueden ser potencialmente confidenciales : <https://support.google>

.com/webmasters/answer/1663419?hl=en&lr=all&rd=2

Eliminar cuentas de Facebook: Contiene indicaciones de cómo eliminar o deshabilitar perfiles de Facebook: https://www.facebook.com/help/250563911970368?helpref=hc_global_nav

Eliminar cuentas de Twitter: Contiene indicaciones de cómo eliminar o deshabilitar perfiles de Twitter: <https://support.twitter.com/articles/15358#>

AccountKiller: Instrucciones para eliminar cuentas y perfiles públicos de sitios y plataformas de redes sociales conocidas: <https://www.accountkiller.com>

Just Delete Me: Directorio de enlaces directos a la opción de eliminar cuentas de los servicios web y plataformas de redes sociales: <http://justdelete.me>

12. A modo de cierre de sesión, recuerda a las participantes que el doxeo revela información que está públicamente disponible sobre ellas; sin embargo, las plataformas de redes sociales y servicios online pueden acceder a mucha más información que esto. Subraya que pueden afianzar su seguridad utilizando contraseñas más robustas, adoptando prácticas más seguras de navegación online y utilizando cifrado para asegurar sus datos.

Referencias

- <https://derechosdigitales.org/anonimato>