



CIBERMUJERES



**Violencia en línea
contra las mujeres**

Hagamos doxxing al troll

**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 Hagamos doxxing al troll	5
Conducir la sesión	6
Parte 1 – ¿Qué es el Doxxing?	6
Parte 2 – Identificar lo/as acosadore/as	7
Parte 3 - Diferentes perfiles, diferentes motivos	8
Parte 4 - Documentar incidentes & amenazas	8
Parte 5 – Preparativos	11
Parte 7 – Herramientas útiles	12
Referencias	13

Hagamos doxxing al troll

- **Objetivos:** Introducir herramientas y actividades centradas en recopilar información sobre acosadore/as. esta información puede ayudar a la hora de tomar decisiones en torno a la privacidad y seguridad en línea.
- **Duración:** 180 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
 - Conceptos básicos de seguridad digital y/o capacitación previa.
 - Navegación más segura¹
 - ¿Qué dicen tus metadatos sobre ti?²
- **Sesiones y ejercicios relacionados:**
 - Navegación más segura³
 - ¿Qué dicen tus metadatos sobre ti?⁴

¹<https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/navegación-más-segura/>

²<https://cyber-women.com/es/activismo-online-más-seguro/qué-dicen-tus-metadatos-sobre-ti/>

³<https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/navegación-más-segura/>

⁴<https://cyber-women.com/es/activismo-online-más-seguro/qué-dicen-tus-metadatos->

- ¡Empecemos a crear un diario de documentación!⁵
- **Materiales requeridos:**
 - Copias impresas de la plantilla de “Diario de documentación” (disponible online)
 - Diapositivas (con los puntos clave descritos a continuación)
 - Computadora y proyector configurados
- **Recomendaciones:** Este ejercicio está recomendado para grupos de defensoras que están viviendo, o vivieron recientemente acoso en línea. aunque no es estrictamente necesario, este ejercicio funciona mejor si el grupo ya participó en la sesión de “¡empecemos a crear un diario de documentación!”. recomendamos que cada participante tenga su propio dispositivo móvil o computadora. quizás quieras dividir la sesión en dos partes puesto que es larga. también puedes hacerla en una sesión, pero con un descanso largo en medio.

Este ejercicio es una adaptación de la actividad desarrollada por Indira Cornelio (SocialTIC) y Phi Requiem (#SeguridadDigital), en colaboración y con el apoyo de “Dominemos las Tecnologías” de APC.

Conducir la sesión

Parte 1 – ¿Qué es el Doxxing?

1. 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.
2. Subraya lo siguiente:

sobre-ti/

⁵<https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/empecemos-a-crear-un-diario-de-documentación/>

El objetivo de este ejercicio no es recomendar el doxxing como una buena práctica (o recomendar métodos ilegales o cuestionables para hacerlo) ya que implica la revelación pública de información personal. Enfatiza que exponer la identidad o información sobre una persona no es necesario. Más bien, lo que se quiere lograr en la sesión es que las participantes aprendan a obtener este tipo de información online para ayudarlas a tomar decisiones fundamentales sobre cómo abordar el abuso y acoso.

3. Finalmente, repasa con ellas prácticas de navegación segura. Parte de este ejercicio implica visitar perfiles y sitios online de los acosadores.

Parte 2 – Identificar lo/as acosadore/as

4. Establezcan las expectativas de cada una para el ejercicio: ¿Qué quieres averiguar de tu acosador/a? Comenta varios posibles motivos de antemano:
 - ¿Quieres descubrir su identidad real?
 - ¿Quieres entender sus motivos?
 - ¿O si están acosando a otras defensoras también?
 - ¿Si están actuando una o varias personas?
5. Puede ser que algunas participantes hayan escuchado maneras de obtener este tipo de información sobre sus acosadore/as, pero aclara que las herramientas y tácticas que van a utilizar en la sesión tiene ciertas limitaciones. Si el grupo ya ha participado en la sesión "¡Empecemos a crear un diario de documentación!", recuérdales la importancia de recopilar pruebas como paso crítico para detectar patrones de acoso y poder denunciarlo. Si aún no han participado en esta sesión, comenta que, más adelante en la sesión, revisarán un método para dar seguimiento a incidentes de acoso.

Parte 3 - Diferentes perfiles, diferentes motivos

6. Comparte algunos casos de mujeres activistas o periodistas y sus experiencias con el acoso en línea. Intenta encontrar casos que sean relevantes a los contextos de las participantes y que muestren perfiles diversos de acosadore/as y motivos.
7. Si alguna participante se siente cómoda compartiendo, puede comentar su propia experiencia al respecto. ¿Cuándo empezó? ¿Quién cree que es? ¿Es una persona conocida para ella? ¿Se les ocurre alguna motivación concreta que pueda tener?
8. Reflexiona sobre los posibles fines y razones que pueda tener la persona acosadora. ¿El acoso se debe a que eres mujer? ¿Porque defiendes derechos de las mujeres/humanos? ¿Has observado este tipo de acoso en tus compañeros varones? Si es así, ¿ocurre de la misma manera o tiene rasgos distintivos?

Parte 4 - Documentar incidentes & amenazas

9. Si el grupo ya participó en la sesión “¡Empecemos a crear un diario de documentación!”, repasa las conclusiones clave y explica cómo la práctica de documentación es un componente importante en obtener información sobre personas acosadoras y tomar decisiones sobre la manera de proceder. Puedes saltar directamente a la Parte 5 - Preparativos
10. Si las participantes aún no han realizado esta sesión, arranca explicando los siguientes puntos que subrayan la relevancia de la documentación a la hora de abordar el acoso en línea:

¿Qué es la documentación?

La documentación, en este contexto, se refiere al abordaje sistemático y organizado de dar seguimiento a un incidente de abuso o acoso que ocurre en nuestro ámbito de trabajo. Básicamente, consiste en archivar pruebas.

Qué es un incidente?

Un incidente es cualquier cosa que ocurre, tanto online como offline, que pueda constituir un abuso o acoso. Que un evento se clasifique como un incidente o no depende, sobre todo, del contexto y circunstancias en que ocurre y la gravedad de su impacto. Por ejemplo, si recibes un correo que parece un intento de phishing - y estás acostumbrada a recibir este tipo de cosas a menudo- quizás, de manera aislada, no sea suficientemente relevante como para considerarlo un incidente; sin embargo, si tu organización está a punto de lanzar una gran campaña y empiezas a recibir una cantidad atípica de correos, ahí sí es probable que podamos considerarlo un incidente y debe ser documentado.

¿Qué es un diario de documentación?

Donde mantienes un registro de los incidentes que ocurren, de manera organizada para facilitar guardar información y evidencias importantes que después puedan servir de referencia. ¿Por qué la documentación es importante? La documentación puede ser útil para volver a ella para relacionar incidentes entre sí durante un periodo de tiempo determinado o entre personas de una misma organización. Puede revelar patrones de abuso u otros tipos de ataques en línea que de otra manera no te hubieras dado cuenta. Estos patrones pueden ayudarte a identificar a adversario/as o establecer conexiones entre diferentes tipos de incidentes y acciones que realizas tú o tu organización. Cuando reportas un abuso en una plataforma de red social, por ejemplo, pueden solicitar durante la investigación pruebas como capturas de pantalla y nombres de perfiles.

11. Ahora puede introducir el cuaderno de documentación a las participantes. Para este ejercicio, puedes utilizar solamente la versión online. Imprime versiones de la plantilla antes del taller y entrégalos al grupo. Véase plantilla a continuación:

Plantilla de diario de documentación (Online)

Fecha

Hora

Resumen del incidente

Plataforma

URL

Captura de pantalla (nombre del archivo o copiar/pegar)

Descripción de la captura de pantalla/contenido

Nivel de riesgo

Pasos de seguimiento

Anotaciones

12. Aclara que estas plantillas sólo brindan un ejemplo de los tipos de información que pueden ser importantes recopilar cuando estás documentando un incidente. Pueden libremente agregar o quitar columnas y campos de la plantilla según vayan creando formatos más específicos que se ajusten a su contexto de trabajo.
13. La mayoría de los campos de las plantillas son fáciles de entender; sin embargo, repásalos de todas maneras, describiendo brevemente qué significa cada uno y qué pretende monitorear.
14. Asegúrate de subrayar el campo de “Nivel de riesgo” ya que este parámetro es muy subjetivo y no tan claro como los demás. Como cada participante u organización define nivel de riesgo es extremadamente específico a su contexto. Puede ser útil parar en este punto y preguntarles a las participantes ejemplos de incidentes que definirían como bajo, medio y alto riesgo. Destaca que deberían considerar el impacto potencial de un incidente (a un nivel personal u organizacional o ambos) cuando estén definiendo un riesgo en este contexto.
15. Las participantes tienen 10-15 minutos para rellenar sus plantillas de documentación individualmente. Pueden rellenar la plantilla con detalles de incidentes actuales o usar ejemplos hipotéticos.

Parte 5 – Preparativos

16. Antes de seguir, es importante recalcar que no entren en los enlaces que pueden llegar a recibir o encontrar cuando están haciendo doxxing de su acosador/a. Estos enlaces pueden ser intentos de phishing (explica este concepto si no la conocen) que buscan engañarte en instalar software malicioso en tus dispositivos. Destaca la gran importancia de evitar entregar información adicional a tu(s) acosadore/a(s); en el mismo sentido, para las participantes que no están enfrentando acoso en la actualidad, es deseable que eviten llamar la atención innecesariamente que pueda desencadenar en acoso.
17. Repasa con las participantes los siguientes pasos para recopilar información sobre sus acosadores/as de manera segura.
 - Recomendamos que reúnan cualquier información que ya pueden tener sobre ello/as y documentar los incidentes en sus cuadernos de documentación.
 - Escojan el navegador web que van a utilizar para su investigación y procuren salir de sus sesiones de cuentas y borrar su historial y cookies. Lo mejor sería utilizar el navegador Tor para esta actividad, si ya han repasado esta herramienta.
 - Quizás quieran considerar crear nuevas identidades o perfiles online para realizar este ejercicio (una cuenta falsa en Facebook, Twitter o Gmail). Recuérdales que tengan cuidado de no usar información que pueda rastrearlas a sus “identidades reales”.
 - Haz énfasis en la importancia de documentar, de tomar anotaciones durante el proceso.
 - Pueden crear una carpeta expresamente para esto en sus computadoras con el fin de recopilar y almacenar cualquier información y pruebas de este ejercicio, como por ejemplo imágenes de avatares, capturas de pantalla, nombres de usuario, cuentas de correo y plataformas de redes sociales, comentarios en foros, comentarios sobre ubicaciones o contactos conocidos.

Parte 7 – Herramientas útiles

18. Ahora puedes empezar a compartir ejemplos de herramientas que puedan ser útiles para su investigación de doxeo. Cuando sea posible, ofrece una copia de tu presentación con toda esta información o un material entregable con una lista de herramientas y enlaces para que puedan volver a ella después para profundizar.
19. Explica cada herramienta y genera el tiempo para que puedan buscarlas en internet y probarlas. Aparte de las que aparecen en la lista a continuación, puedes agregar otras que conoces que consideres que puedan ser útiles o relevantes:
 - Considera cifrar tus discos.
 - Deja Google y usa StartPage⁶ o DuckDuckGo⁷.
 - Recomienda usar Tails⁸ o cuando no sea posible, usar el navegador Tor⁹.
 - Búsqueda avanzada en Twitter¹⁰.
 - Checa <http://whois.net> para buscar información vinculada a un sitio web como quién es propietario/a del dominio.
 - Búsqueda inversa de imágenes en Google¹¹ para rastrear imágenes y fotos que hayas podido recibir.
 - Herramientas de metadatos en caso de que hayas recibido imágenes o fotos:
 - MetaShield¹²
 - MetaPicz¹³

⁶<https://startpage.com>

⁷<https://duckduckgo.com>

⁸<https://tails.boum.org>

⁹<https://www.torproject.org>

¹⁰<https://twitter.com/search-advanced>

¹¹<https://images.google.com/>

¹²<https://www.elevenpaths.com/technology/metashield/index.html>

¹³<http://metapicz.com>

-
- Social Mention (“Mención social”)¹⁴;
 - Follower Wonk¹⁵;
 - NameCheck (“Verificar nombres”)¹⁶;
20. Explica que hay maneras de construir sistemas simples de monitoreo online que funcionan especialmente bien cuando queremos seguirle la pista a ciertos nombres de perfil, usuario o hashtag.
- IFTTT¹⁷ – explica cómo permite a las usuarias conectar Twitter con Google Drive para monitorear tweets y menciones vinculadas a cierta cuenta de usuario/a o hashtag.
 - Google Alerts¹⁸
 - Tweetdeck¹⁹
21. Dependiendo del tiempo que tengan, las participantes pueden realizar su investigación durante el taller o hacerlo para la siguiente sesión. Sea de una manera u otra, recuérdales que será útil - una vez que hayan recopilado información - dar un paso atrás y mirar todos los datos que han reunido:
- ¿Observan patrones emergentes?
 - ¿Qué revela la información sobre su acosador/a?
 - Quizás puedan hasta predecir futuros blancos potenciales o tipos de ataques.

Referencias

- <https://www.apc.org/es/pubs/issue/como-evitar-convertirse-en-una-victima-del-ciberac>

¹⁴<http://socialmention.com>

¹⁵<https://moz.com/followerwonk>

¹⁶<https://namechk.com>

¹⁷<https://ifttt.com>

¹⁸<https://www.google.com/alerts>

¹⁹<https://tweetdeck.twitter.com>

- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Lidiar_con_Trols
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Bots_contra_trols