INSTITUTE FOR WAR & PEACE REPORTING

IWPR

CIBERMUJERES

Currícula de Capacitación en Seguridad Digital Holística para Defensoras de Derechos Humanos

Seguridad, Concientización y Acción para Defensoras de Derechos Humanos

Esta currícula fue creada e implementada por IWPR como parte del proyecto "Seguridad, Concientización y Acción" (Safety, Awareness and Action -SAWA-) y financiada por la Oficina de Democracia, Derechos Humanos y Trabajo ("Bureau of Democracy, Human Rights and Labor -DRL-") del Departamento del Estado de EEUU.

Agradecimientos

Esta currícula fue creada e implementada por el IWPR como parte del proyecto "Seguridad, Concientización y Acción" (Safety, Awareness and Action -SAWA-) y financiada por la Oficina de Democracia, Derechos Humanos y Trabajo ("Bureau of Democracy, Human Rights and Labor -DRL-") del Departamento del Estado de EEUU.

Autoras
El contenido original de esta currícula fue desarrollado por Alma Ugarte Pérez e Indira Cornelio Vidal.

Coordinación y Sistematización
Alma Ugarte Pérez, Indira Cornelio Vidal, Dhaniella Falk.

Educación y Localización
Nicholas Sera-Leyva

Traducción al español
Nadège Lucas Pérez

Diseño
Sandra Ordóñez de la Open Technology Fund

Revisión entre pares y Colaboradoras
Azza Sultan, Carol Waters, Dalia Othman de Tactical Technology Collective, Erika Smith de la Association for Progressive Communications, Gigi Alford, Jennifer Schulte, Laura Cunningham, Lindsey Andersen y Megan DeBlois de Internews.

Algunas sesiones y contenidos adaptados para esta currícula fueron desarrollados originalmente por:
Association for Progressive Communications, Tactical Technology Collective, Fundación Karisma, Mujeres Al Borde, Elis Monroy de Subversiones Collective, Danah Boyd, Mariel García, Alix Dunn, Spyros Monastiriotis y Phi Requiem.
La atribución para estos contenidos y sesiones están señaladas debajo de sus respectivos títulos.

ÍNDICE DE CONTENIDOS

Módulos de Capacitación

1 | Ejercicios para fortalecer la confianza

2 | Repensando nuestra relación con las tecnologías

3 | Principios básicos de seguridad digital | Parte 1

4 | Privacidad

5 | Activismo online más seguro

6 | Celulares más seguros

7 | Anonimato

8 | Cifrado

9 | Principios básicos de seguridad digital | Parte 2

10 | Violencia en línea contra las mujeres

11 | Sexting

12 | Buscando la mejor solución

13 | Planeando con anticipación

14 | Auto-cuidado

15 | Ejercicios de cierre y evaluación

Apéndices

INTRODUCCIÓN

Introducción a Cibermujeres

A lo largo de los últimos años, han surgido numerosos esfuerzos para crear recursos, metodologías y prácticas mejoradas para capacitaciones en seguridad digital; sin embargo, pocos resultados han incorporado una perspectiva de género de manera consolidada y consistente. Más recientemente, gracias a los esfuerzos dentro de los movimientos de mujeres y feministas en todo el mundo, ha empezado a emerger un abanico de contenidos sobre seguridad digital enfocadas en temas de género. Aún así, persiste la falta de coordinación en la comunidad de seguridad digital para alimentar esta colección de recursos de una manera estratégica y respondiendo a los contextos.

Con este fin, IWPR ha construido la currícula Cibermujeres con la intención de resonar las técnicas y prácticas desarrolladas por defensoras de derechos humanos (WHRDs) que lideran iniciativas de capacitación en seguridad digital en la región de Latinoamérica y el Caribe (LAC). Basándonos en la experiencia del trabajo de estas mujeres, hemos creado, desde un abordaje co-construido y desde una perspectiva de género, este contenido original para formadoras en seguridad digital que trabajan con defensoras de las libertades y derechos.

Para evitar duplicar esfuerzos, identificamos materiales ya existentes que respondieron a las necesidades y contextos de las defensoras: por ejemplo, algunos contenidos de la currícula de LevelUp o recursos desarrollados por organizaciones como Tactical Technology Collective (TTC) y Association for Progressive Communications (APC). Dichos contenidos han sido incorporados directamente en la currícula, con su respectiva atribución y créditos. Sin embargo, el valor y aporte esencial de este material reside en los módulos y las recomendaciones creadas específicamente para esta currícula con el fin de brindar experiencias de aprendizaje hechas a medida para los contextos de las defensoras que trabajan en entornos de alto riesgo.

Cómo utilizar la Currícula de Cibermujeres

Esta currícula ha sido diseñada tomando en cuenta dos tipos de perfiles: por un lado, formadoras que buscan conducir capacitaciones sobre seguridad digital con perspectiva de género a grupos de mujeres; por otro lado, mujeres que han recibido una capacitación y quieren transmitir este conocimiento sobre seguridad digital a sus redes de compañeras/os y activistas. El conjunto completo de sesiones no es relevante para todos los públicos, así que te animamos a identificar y enfocar las que cobran valor y sentido para la comunidad con la que trabajas.

Cibermujeres incluye juegos interactivos, materiales gráficos y audiovisuales, además de guías para apoyar a las facilitadoras. Los módulos pueden utilizarse por separado o combinados para diseñar un taller completo. Esta estructura modular permite a las formadoras seleccionar contenidos específicos que se ajustan a las necesidades de las participantes de la capacitación o, si así prefieren, también pueden seguir las secuencias (rutas) de módulos sugeridas. Si quisieras cubrir toda la currícula de principio a fin, necesitarías aproximadamente 10 días completos; para quienes quieran facilitar una capacitación de este tipo, recomendamos espaciar las sesiones a lo largo de seis meses. Con este abordaje, las participantes tendrán suficiente tiempo para integrar, de manera eficaz, nuevas técnicas y herramientas en sus prácticas personales de seguridad digital antes de avanzar a desarrollar nuevas habilidades.

Además, como parte de este enfoque en seguridad holística, la currícula incorpora contenidos específicos sobre auto-cuidado feminista y reconoce la violencia de género, tanto simbólica como online. El objetivo de estas sesiones es reforzar el sentido de apropiación y control de las participantes sobre su seguridad e identidades. Por lo tanto, es importante que sean integrados estos temas transversales a lo largo de las capacitaciones como oportunidades para la acción y reflexión colectiva e individual, y no como módulos aislados.

Hay muchas actividades y ejercicios incluidos en esta currícula: algunas son para fortalecer la confianza –recomendamos empezar por aquí, al principio de todo–; otras sirven para romper el hielo al arrancar cada día del taller. Finalmente, algunas actividades están diseñadas para fortalecer ciertos contenidos de capacitación y tienen un orden determinado. La currícula también incluye materiales complementarios para dar seguimiento a lo largo de los seis meses de duración sugerida.

Una perspectiva feminista en la creación de esta currícula

Como comentamos anteriormente, esta currícula integra una visión holística sobre la seguridad para defensoras de derechos humanos, incluyendo la "tríada" seguridad digital, seguridad física y auto-cuidado. Cabe mencionar que nos enfocamos en el componente de seguridad digital. Para un abordaje más transversal y sensible a temas de género y más feminista, esta currícula fue producida con los siguientes valores y principios medulares en mente – animamos enfáticamente que las formadoras y facilitadores las tomen en cuenta cuando diseñen sus talleres utilizando esta currícula:

Mujeres participantes y mujeres formadoras

Primero, y sobre todo, los contenidos de Cibermujeres están diseñados para apoyar la confianza y autoestima entre mujeres en el contexto del taller. Las participantes suelen venir de entornos –tanto física como emocionalmente– de alto estrés y ansiedad; las defensoras de derechos humanos suelen ser el blanco de acoso y violencia online y offline. Es esencial que perciban la capacitación como un espacio seguro donde puedan sentirse cómodas compartiendo sus miedos, dudas y emociones, y que puedan participar e interactuar entre ellas activamente. Por lo tanto, esta currícula está dirigida a **mujeres formadoras trabajando con participantes mujeres.** Sin embargo, también alentamos que formadores hombres y diversos revisen esta currícula y sus principios fundacionales para adaptar mejor su praxis en talleres con grupos mixtos.

Modelos femeninos y feministas

Esta currícula ha sido creada con un enfoque específico en el intercambio de experiencias personales de ataques digitales –tal cual han sido vividas por las defensoras, activistas y periodistas– a través de testimonios que empoderen. Reconociendo que no todas las mujeres en el taller van a definirse como feministas, el abordaje que proponemos del proceso de capacitación se centra en crear conciencia sobre la violencia en línea contra las defensoras; primero subrayando las diferencias entre los ataques dirigidos hacia hombres y mujeres activistas; después, proporcionando ejemplos de violencia de género en línea (ej. en plataformas de redes sociales) como una manera de ayudar a las mujeres a identificar la violencia que quizás ya hayan afrontado en estos espacios.

Como parte de esta metodología, presentamos estudios de casos cercanos al día a día de las mujeres, facilitando que las participantes puedan relacionarse a diferentes situaciones y comprender la relevancia que cobran en sus propios contextos. Nos dimos cuenta que este abordaje empodera a las mujeres y las anima a practicar, de manera más consistente, nuevas habilidades y transmitir a otras personas consejos sobre seguridad digital.

¡Mi cuerpo, mis dispositivos, mi decisión!

Las principales ideas, información y prácticas compartidas en esta currícula se arraigan en promover la **autonomía digital**. El énfasis del "pensamiento estratégico sobre la seguridad digital" es el núcleo del diseño de esta guía: compartir conceptos de seguridad digital con las participantes en vez de entrenarlas en una lista de herramientas. Invertimos una gran parte del tiempo a presentar conceptos de seguridad digital como el cifrado, el anonimato, la privacidad y el software open-source, antes de capacitar en las herramientas relacionadas. Apoyar a las mujeres a desarrollar su propia comprensión de estos conceptos ayuda a que se lleven la información necesaria para tomar sus propias decisiones sobre qué herramientas son mejores para ellas.

Análisis de riesgos con perspectiva de género de género en plataformas de redes sociales

Utilizamos ejemplos de vídeos de *Youtube*, mensajes en diferentes plataformas de redes sociales y resultados de otras sesiones de capacitación con el objetivo de crear un espacio seguro para la discusión y reflexión sobre violencia de género que surge en una dimensión de tecnologías digitales. Específicamente, la gran parte de lo mencionado converge en el módulo de "Violencia en línea contra mujeres"; de igual manera, el ejercicio "Modelo de riesgos con perspectiva de género" incluido en el módulo "Buscando la mejor solución" se centra en compartir experiencias e identificar las vulnerabilidades que las participantes enfrentan, no sólo por ser mujeres, sino por realizar actividades críticas a los roles hegemónicos: activismos, comunicación, organización, creación...

Auto-cuidado feminista & Defensa personal digital

Como parte de un abordaje holístico de la seguridad, esta currícula contempla el bienestar emocional y el auto-cuidado como elementos vitales de la seguridad para las defensoras; en este mismo sentido, como parte del enfoque de la autonomía digital, hay sesiones específicas –como la sesión "Modelo de riesgos con perspectiva de género"– que tienen la intención de ayudar a las participantes a prepararse para y reaccionar ante ataques digitales. Esta guía es un esfuerzo para brindar información a las participantes para que identifiquen y exploren diversas estrategias para su defensa personal digital; éstas incluyen, pero no se reducen a: separar la esfera personal de la pública, crear identidades online, "hacer doxxing al troll", cifrar comunicaciones y documentar incidentes digitales. Preparar a las participantes con una mejor comprensión sobre su entorno online –en las plataformas que utilizan y los riesgos asociados a ellas– nos permite empoderarlas en desarrollar hábitos robustos de seguridad digital que puedan formar parte de una práctica holística de auto-cuidado.

PLANEANDO RECURSOS

Diagnóstico y evaluación antes de empezar la capacitación

Realizar un diagnóstico antes de diseñar la capacitación es crucial. Obtener una comprensión profunda sobre las necesidades en seguridad digital de las participantes ayuda a asegurar una capacitación efectiva y una experiencia de aprendizaje adaptada a sus contextos y objetivos. Conocer la experiencia que tienen las participantes con las tecnologías -cómo las utilizan y se comunican con ellas- tiene un impacto significativo en el espectro de contenidos que vamos a cubrir en nuestro taller.

Evaluando necesidades y motivaciones

Idealmente, las formadoras llevarán a cabo una evaluación de necesidades antes de la capacitación, trabajando con las participantes o con una representante de su organización o colectivo. Toma en cuenta que, más allá de objetivamente evaluar sus necesidades, será importante también comprender sus motivaciones en participar en la capacitación: ¿están proactivamente buscando fortalecer su propia resiliencia o están solicitando apoyo en respuesta a incidentes recientes o aún en curso? Además, en un sentido más pragmático, contempla que la cantidad de contenidos en las sesiones tiene que concordar con el objetivo de las personas o el grupo y con las habilidades de las mismas. El conjunto de saberes colectivos de las participantes también será un factor determinante.

Si tienes la oportunidad de interactuar y comunicarte con las participantes en más profundidad antes del taller, aquí sugerimos una serie de preguntas que puedes plantear para aprender más sobre ellas y/o el grupo con el que trabajan:

- ¿Cuál es la trayectoria del grupo?
- ¿Cómo está configurado el grupo? ¿Cómo se organiza?
- ¿Cuáles son sus objetivos, agendas y actividades?
- ¿Cuáles son algunas de sus prácticas relacionadas con las tecnologías? ¿Cómo y desde dónde acceden a Internet?
- ¿Qué tipo(s) de computadoras y/o dispositivos móviles utilizan? ¿Usan dispositivos separados para su actividad personal y profesional?
- ¿Qué sistemas operativos utilizan?
- ¿Con qué movimientos y/o grupos colaboran? Puede ser como representante de su organización (ej. como miembros de una coalición o red) o a nivel personal como activistas independientes.
- ¿Han experimentado incidentes o amenazas directas hacia su seguridad física y/o digital? Ello puede estar relacionado con sus dispositivos, infraestructura y posesiones, cuentas online y/o agresiones físicas.

Herramienta de seguridad digital y capacidades (DISC)

Si tienes la oportunidad de entablar un proceso de evaluación y diagnóstico integral con las participantes antes del taller, la herramienta DISC incluida en esta currícula puede ser útil para ti. Es un recurso creado por IWPR y es utilizado ampliamente en procesos de diagnóstico y evaluación pre-capacitación.

La herramienta DISC es un cuestionario que utiliza un mecanismo de puntuación cuantitativa para medir el nivel de conocimientos y habilidades que tienen las participantes en temas de seguridad digital. También brinda información cualitativa sobre las fortalezas y ámbitos que pueden mejorarse a un nivel más detallado y enfocado en las praxis. Si vas a estar trabajando de manera constante con las participantes (por ej, sesiones durante 6 meses), la herramienta DISC puede ser útil para monitorear avances de aprendizaje y comprensión.

[La herramienta DISC completa puede encontrarse aquí (Apéndices)]

Estrategias alternativas de evaluación y diagnóstico

Si no puedes realizar directamente un diagnóstico antes de la capacitación, ni obtener respuestas a estas preguntas comentadas anteriormente, todavía puedes conseguir bastante información sobre las trayectorias de las participantes a partir de sus contextos y circunstancias:

- Por ejemplo, si conoces a mujeres y organizaciones activistas que están haciendo un trabajo parecido en la misma región que los grupos con los que vas a trabajar, es probable que hayan enfrentado riesgos y/o ataques similares.

- Además, posiblemente haya amenazas o incidentes que correlacionan con el tipo de trabajo que las participantes realizan (y los lugares donde actúan). Si vas a estar capacitando abogadas que acompañan a otras defensoras o periodistas que denuncian casos de corrupción gubernamental, puedes investigar las tácticas que actores estatales y no estatales han aplicado contra individuos, particularmente hacia mujeres, que operan en el mismo país y en ámbitos parecidos.

Ejemplos de rutas de capacitación

Aunque nos damos cuenta que el contenido final de la capacitación se basará en el diagnóstico que cada formadora realice sobre el grupo con el que va a trabajar, compartimos varias rutas a modo de ejemplo.

Las rutas a continuación se organizan por duración (en días) y por nivel de habilidades. Otros parámetros entran en juego a la hora de planear la capacitación, pero generalmente el factor tiempo es el más crítico:

El tiempo del que dispones determina, en última instancia, cuánto contenido puedes cubrir en un taller; el conjunto de saberes de las participantes también será un factor determinante.

Es más probable que sepas de antemano de cuánto tiempo dispones antes de saber otros factores como el espacio donde se va a realizar el taller, el número de participantes o su nivel de conocimientos/experiencias.

Rutas de ejemplo para talleres de un día o un día y medio

Taller introductorio de un día y medio sobre evaluación de riesgos

Tiempo aprox. requerido: 10 horas
Esta ruta está diseñada para un taller introductorio de seguridad digital de un día y medio para un grupo de defensoras de derechos humanos o un colectivo de mujeres, orientada principalmente a la evaluación general de riesgos. Idealmente, el resultado de este taller es que las participantes puedan identificar más fácilmente riesgos percibidos y articulen de una manera más clara sus necesidades en torno a la seguridad digital.

Esta ruta incluye sesiones sobre principios básicos de seguridad digital, prácticas de auto cuidado y técnicas para documentar y actuar ante casos de abuso y/o amenazas. Para este escenario, será necesario que la formadora diseñe una estrategia de seguimiento que aborde los resultados que salgan en las evaluaciones de riegos de las participantes.

1. Ejercicio: Las reglas del juego (Ejercicios para fortalecer la confianza)

2. Ejercicio: El bingo de las defensoras (Ejercicio para fortalecer la confianza)

3. Sesión: Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)

4. Ejercicio: ¿En quién confías? (Ejercicio para fortalecer la confianza)

5. Sesión: Nuestros derechos, nuestra tecnología (Repensar nuestra relación con las tecnologías)

6. Ejercicio: Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

7. Ejercicio: Construyendo un auto-cuidado feminista (Auto-cuidado)

8. Sesión: Creando contraseñas más seguras (Principios básicos de seguridad digital | Parte 1)

9. Sesión: Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

10. Sesión: Navegación segura (Principios básicos de seguridad digital | Parte 1)

11. Sesión: Privacidad (Privacidad)

12. Sesión: Celulares | Parte 1 (Celulares más seguros)

13. Sesión: ¡Empecemos a crear un diario de documentación! (Violencia en línea contra mujeres)

14. Ejercicio: Flores feministas (Ejercicios de cierre y evaluación)

Capacitación en concientización (1 día) para defensoras que afrontan acoso online

Tiempo aprox. requerido: cinco horas
Esta ruta está diseñada para un taller introductorio de seguridad digital de un día para defensoras de derechos humanos que empiecen a afrontar incidentes de acoso online. Idealmente, el resultado de este taller es que las participantes puedan articular de una manera más clara sus necesidades en torno a la seguridad digital y puedan identificar más ágilmente indicadores de advertencia o patrones de violencia de género en línea.

Esta ruta incluye sesiones sobre cómo definir la seguridad a un nivel personal, prácticas básicas de seguridad digital y reconocimiento de patrones de abuso y acoso.

1. Ejercicio: Las reglas del juego (Ejercicio para fortalecer la confianza)

2. Ejercicio: El bingo de las defensoras (Ejercicio para fortalecer la confianza)

3. Sesión: Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)

4. Sesión: Creando contraseñas más seguras (Principios básicos de seguridad digital | Parte 1)

5. Ejercicio: Violencia simbólica (Violencia en línea contra mujeres)

6. Ejercicio: ¡Empieza la función! (Sexting)

7. Sesión: Sexting (Sexting)

8. Ejercicio: Nuestras reflexiones (Auto-cuidado)

Capacitación en concientización (1 día) para defensoras que afrontan acoso online

Tiempo aprox. requerido: cinco horas
Esta ruta está diseñada para un taller de un día para defensoras de derechos humanos que están enfrentando ahora, en el presente, incidentes de acoso en línea, y que necesitan ayuda para desarrollar protocolos de seguridad y estrategias de respuesta. Idealmente, el resultado de este taller es que las participantes puedan articular de una manera más clara sus necesidades en torno a la seguridad digital, se sientan más en control de su entorno de riesgos personales y sean capaces de desarrollar, para ellas mismas, protocolos de seguridad que respondan a sus contextos.

Esta ruta incluye sesiones sobre cómo definir la seguridad a un nivel personal, prácticas básicas de seguridad digital y evaluación de riesgos con perspectiva de género.

1. Ejercicio: Las Reglas del juego (Ejercicio para fortalecer la confianza)

2. Sesión: Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)

3. Ejercicio: ¿En quién confías? (Ejercicio para fortalecer la confianza)

4. Ejercicio: Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

5. Sesión: Privacidad (Privacidad)

6. Ejercicio: Hagamos doxxing al troll (Violencia en línea contra mujeres)

7. Ejercicio: Construyendo un auto-cuidado feminista (Auto-cuidado)

Rutas de ejemplo para talleres de tres días

Capacitación introductoria de tres días

Tiempo aprox. requerido: 15 horas
Esta ruta está creada para un taller de tres días con defensoras principiantes que aún no tienen, o muy poca, familiaridad con prácticas de seguridad digital. Introduciremos prácticas básicas de seguridad digital y evaluación de riesgos con un énfasis explícito en estrategias de auto-cuidado. Esta ruta es apropiada para trabajar con organizaciones o con un grupo mixto de defensoras que participan en diferentes colectivos o países dentro de la misma región. Además, esta ruta preparará al grupo para una segunda capacitación de nivel intermedio (*véase el ejemplo de "Capacitación nivel intermedio de tres días*" a continuación) aunque también puedan realizar esta capacitación por separado.

1. Ejercicio: Las reglas del juego (Ejercicio para fortalecer la confianza)

2. Ejercicio: El bingo de las defensoras (Ejercicio para fortalecer la confianza)

3. Sesión: Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)

4. Ejercicio: ¿En quién confías? (Ejercicio para fortalecer la confianza)

5. Sesión: Nuestros derechos, nuestra tecnología (Repensar nuestra relación con las tecnologías)

6. Sesión: ¿Cómo funciona Internet? (Principios básicos de seguridad digital | Parte 1)

7. Ejercicio: Flores feministas (Ejercicios de cierre y evaluación)

8. Ejercicio: Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

9. Ejercicio: El acto del NO (Auto-cuidado)

10. Sesión: Creando contraseñas más seguras (Principios básicos de seguridad digital | Parte 1)

11. Sesión: Navegación segura (Principios básicos de seguridad digital | Parte 1)

12. Sesión: Malware & Virus (Principios básicos de seguridad digital | Parte 1)

13. Ejercicio: Construyendo un auto-cuidado feminista (Auto-cuidado)

14. Sesión: Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

15. Sesión: ¿Qué dice tus metadatos sobre ti? (Activismo online más seguro)

16. Ejercicio: Marco Polo (Celulares más seguros)

17. Sesión: Celulares | Parte 1 (Celulares más seguros)

18. Sesión: Multitudes interconectadas (Privacidad)

19. Sesión: Privacidad (Privacidad)

20. Sesión: ¡Empecemos a crear un diario de documentación! (Violencia en línea contra mujeres)

Capacitación nivel intermedio de tres días

Tiempo aprox. requerido: 15 horas

Esta ruta es un taller de seguimiento de tres días con defensoras que ya participaron en una capacitación introductoria (véase "Capacitación introductoria de tres días" más arriba). Es considerablemente más técnico que el nivel anterior, con un enfoque a aplicaciones prácticas de conceptos de seguridad digital, además del desarrollo de habilidades de pensamiento crítico para tomar decisiones fundamentadas a la hora de escoger herramientas digitales. También profundiza más en temas como mujeres y tecnologías, privacidad, cifrado y anonimato.

Si vas a trabajar con participantes que pertenecen a una misma organización, esta capacitación les permitirá diseñar estrategias para empezar a compartir conocimientos con sus compañera/os de la organización y crear juntas planes y protocolos de seguridad.

1. Ejercicio: Dulce o truco (Ejercicio para fortalecer la confianza)

2. Ejercicio: Yo decido (Buscando la mejor solución)

3. Sesión: Her-Story (las historias de las mujeres) en las tecnologías (Repensar nuestra relación con las tecnologías)

4. Ejercicio: ¡Pregúntame cualquier cosa! (Privacidad)

5. Sesión: Apps & Plataformas online: ¿Amigo/a o enemigo/a? (Privacidad)

6. Sesión: Campañas online más seguras (Activismo online más seguro)

7. Sesión: Celulares | Parte 2 (Principios básicos de seguridad digital | Parte 1)

8. Sesión: Introducción al cifrado (Cifrado)

9. Sesión: Comunicación cifrada (Cifrado)

10. Ejercicio: La caldera (Ejercicios de cierre y evaluación)

11. Sesión: Almacenamiento & Cifrado (Principios básicos de seguridad digital | Parte 2)

12. Ejercicio: Amistad secreta (Anonimato)

13. Sesión: Anonimato (Anonimato)

14. Sesión: (Toma de) Decisiones sobre seguridad digital (Buscando la mejor solución)

15. Sesión: Planes y protocolos de seguridad en organizaciones (Planeando con anticipación)

16. Ejercicio: Carta de amor a mi misma (Auto-cuidado)

Capacitación avanzada de tres días

Tiempo aprox. requerido: 12 horas
Esta ruta está creada para un taller de tres días con defensoras que ya participaron en una formación de nivel introductorio e intermedio (véase ejemplos anteriores) y que están preparadas para una experiencia más avanzada.

Este taller se orienta más hacia el desarrollo de tácticas y prácticas en torno a herramientas específicas, más que en el ámbito de conocimientos conceptuales. Hace énfasis en aplicar el pensamiento crítico y toma de decisiones en contextos reales (lo que te permite, como formadora, evaluar de manera más integral los avances del grupo).

1. Ejercicio: ¡Adivinanzas! (Ejercicios de cierre y evaluación)

2. Sesión: Sitios web más seguros (Activismo online más seguro)

3. Ejercicio: ¡Más identidades online!(Anonimato)

4. Sesión: ¡Empecemos de nuevo! (Principios básicos de seguridad digital | Parte 2)

5. Ejercicio: Hagamos doxxing al troll (Violencia en línea contra mujeres)

6. Sesión: Planes y protocolos de seguridad digital: replicar después del taller (Planeando con anticipación)

7. Ejercicio: Tacto con amor (Auto-cuidado)

8. Ejercicio: Yincana DigiSec (Ejercicios de cierre y evaluación)

Módulos de Capacitación

Ejercicios para fortalecer la confianza

Las Reglas del Juego

Objetivo(s): construir colectivamente acuerdos de convivencia y participación para el taller - "las reglas del juego".

Módulo: Ejercicios para fortalecer la confianza

Formato: Ejercicio

Nivel de habilidades: Básico

Duración: 8-10 minutos

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- Dulce o truco (Ejercicio para fortalecer la confianza)
- El bingo de las defensoras (Ejercicio para fortalecer la confianza)

Materiales requeridos:
- Rotafolio (o pizarrón)
- Marcadores
- Stickers de colores (tres colores – idealmente rojo/rosa, amarillo y verde)

Recomendaciones:
- Parte 2 del ejercicio– “Semáforo” - funciona mejor si las participantes tienen etiquetas con sus nombres sobre los que se pegarán pegatinas de colores.

Conducir la sesión:

En cualquier proceso de capacitación, aunque suele haber ya una relación establecida entre las participantes y con la facilitadora, es esencial establecer colectivamente acuerdos de convivencia (que llamamos "reglas del juego") para cultivar un entorno agradable y respetuoso.

Las experiencias y contextos culturales de cada mujer son únicos. Lo que puede parecer completamente inofensivo para alguien, pueda ser interpretado de manera totalmente diferente para las demás. Construir juntas acuerdos de convivencia ayuda asegurar que la capacitación albergue diferentes puntos de vista y zonas personales de confort; por ejemplo, algunas mujeres pueden sentirse incómodas con el contacto físico, mientras otras lo consideren un medio de auto-expresión. Otro ejemplo: algunas participantes que provienen de un contexto educativo más tradicional pueden llegar a pedir permiso para ir al baño mientras para otras sea totalmente natural levantarse en mitad del taller e ir.

Esta sesión te ayudará a generar estos acuerdos colectivos de convivencia, reconociendo las preferencias de las participantes para que puedan sentirse cómodas, y, como consecuencia, puede dar lugar a mayor receptividad en el taller.

Parte 1 – Las reglas del juego

1. Explica brevemente el contexto anterior a las participantes y pídeles que den ejemplos de acuerdos de convivencia que consideren importantes y esenciales para su bienestar en el taller. Puedes empezar dando ejemplos como "no necesitamos pedir permiso para ir al baño" o "no compartiremos nada sobre este taller en plataformas de redes sociales sin el consentimiento de las demás"

2. Anota cada acuerdo que se comparte en el grupo en el rotafolio o pizarrón conforme vayan saliendo. Una vez que consideres que sean suficientes, lee en voz alta cada acuerdo - pregúntales a las participantes su opinión. Al menos que ya hayan sido abordados en los ejemplos del principio o las aportaciones de las participantes, puede ser útil comentar acuerdos sobre el uso de dispositivos (computadoras y celulares) en las sesiones.

3. Comenta que los acuerdos se colocarán en un lugar visible durante todo el taller y que pueden ser modificados en la medida que se discutan y consensúen en grupo. Asegúrate de ofrecer a las participantes la opción de hacer sugerencias directamente a ti o de manera anónima en caso de que no se sientan cómodas de hacerlo abiertamente.

Parte 2 – "Semáforo"

4. Puede ser que determinados acuerdos en tu lista suscite distintos niveles de confort en el grupo. Para estos acuerdos, por ejemplo relacionado con el contacto físico o la toma de fotos, puedes ofrecer a las participantes una manera de indicar el nivel personal de confort hacia el resto del grupo.

5. Reparte los stickers de colores a cada participante, asegúrate de que cada una tenga varios de cada color. Explica que para algunos de los acuerdos de convivencia (indica cuáles) de la lista, el grupo realizará un pequeño ejercicio llamado "Semáforo".

6. Usa el siguiente ejemplo: "Antes de realizar un contacto físico con otra participante, nos aseguraremos antes que se sientan cómodas". El grupo asignará valores a cada sticker de color, por ejemplo:

- Rojo/Rosa: “El contacto físico me incomoda un poco. Por favor, respeta mi espacio.”
- Amarillo: “No me molesta el contacto físico, pero pregunta primero”
- Verde: “No me molesta el contacto físico para nada”

7. Las participantes escogen un sticker para si mismas según su relación de confort y lo colocará en su etiqueta de nombre. Las participantes no tienen que compartir qué color escogieron porque se podrá ver en sus etiquetas.

8. Escribe la leyenda de colores y significados para cada acuerdo en una nueva hoja del rotafolio o en el pizarrón. No debería haber más de dos o tres. Si hay más, agreguen una letra para distinguirlas (por ejemplo, "c" para contacto, "f" para fotos)

El bingo de las defensoras

Objetivo(s): la facilitadora y las participantes se presentan a través de un juego interactivo para romper el hielo y conocerse un poco más allá de sus nombres.

Módulo: Ejercicios para fortalecer la confianza

Formato: Ejercicio

Nivel de habilidades: Básico

Duración: 12-15 minutos (dependiendo del tamaño del grupo)

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- Dulce o truco (Ejercicio para fortalecer la confianza)

Materiales requeridos:
- Hojas de bingo para cada participante (ya rellenadas con sus nombres)
- Tarjetas índice en blanco
- Lapiceros/plumas/bolígrafos (suficientes para todas las participantes)
- Opcional: Marcadores y etiquetas adherentes en blanco (para escribir nombres)

Conducir la sesión:

Acordarse de los nombres e identificar caras puede ser más difícil para algunas personas. Este ejercicio para "romper el hielo" ayudará a las participantes recordar estos detalles y también llegar a conocer a sus compañeras del taller.

1. Cada participante escribe su nombre en las tarjetas índice. Junta todas cuando hayan terminado.
2. Entrega una hoja de bingo a cada participante (sus nombres ya estarán escritos en sus hojas). Opcionalmente, podrás incluir tu nombre en la pizarra. Véase el ejemplo a continuación.

Ejemplo de una hoja de bingo ya preparada:

Alma	Kim	Sophie
Heidi	Cristina	Roua
Marcela	Tippy	Indira
Anaiz	Lulu	Maria

- Explica el funcionamiento al grupo:
    - Lee en voz alta, uno por uno, las tarjetas índice que las participantes rellenaron con su nombre;
    - Conforme vayas leyendo los nombres, las participantes los rodearán si aparece en su hoja de bingo;
    - La primera participante en rodear una fila completa de nombres (en horizontal o vertical) gritará "¡Bingo!" y será proclamada la ganadora.
- Esta persona lee en voz alta el primer nombre de la fila ganadora - la participante con dicho nombre se levanta, repite su nombre y comparte algo con el grupo (escoge de antemano qué se compartirá y coméntalo a la hora de presentar el juego; por ejemplo: qué te gusta hacer en tu tiempo libre, cuál es tu canción, película o comida favorita, etc.)

5. Se repite el proceso para todos los nombres de la fila. Conforme se leen los nombres en voz alta, aparta la tarjeta índice correspondiente de la pila.

6. Una vez que la ganadora haya leído en voz alta todos los nombres, agradece su participación y, después, lee en voz alta los nombres de las tarjetas índice restantes para que todas las participantes tengan la oportunidad de presentarse.

7. Ahora te toca a ti. Repite tu nombre al grupo y comparte algo sobre ti. Cierra el ejercicio recordando al grupo que están todas empezando una aventura juntas y que (re)conocerse entre sí es vital para el camino compartido.

Opcional: *al final del ejercicio, entrega a cada participante un sticker en blanco y un marcador para que anoten su nombre. No sólo sirve para que se acuerden de los nombres de las compañeras sino te ayuda a ti en el proceso de facilitación.*

Dulce o truco

Objetivo(s): la facilitadora y las participantes se presentan a través de un juego interactivo para romper el hielo y conocerse un poco más allá de sus nombres.

Módulo: Ejercicios para fortalecer la confianza

Formato: Ejercicio

Nivel de habilidades: Básico

Duración: 5 a 8 minutos (dependiendo del tamaño del grupo)

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- Las Reglas del Juego (Ejercicio para fortalecer la confianza)

Materiales requeridos:
- 1 o 2 bolsas de dulces
- Opcional: diferentes tipos de dulces o con distintos envoltorios

Conducir la sesión:

Ofrece dulces a todas las personas del grupo, indicando que puedan tomar todas las que quieran. Algunas se llenarán más las manos que otras. Tú también puedes tomar.

Ahora viene el truco: por cada dulce que te llevaste, comparte un detalle o cualidad sobre ti. Cosas como:
- Un deseo o meta personal
- Algo que disfrutas de tu trabajo
- Un país o lugar que quieres visitar

Opcional: si hay diferentes tipos de dulces, puedes asignar cada clase a una categoría. Por ejemplo:

- *Envoltorio rojo = deseo o meta personal*
- *Envoltorio verde = algo que disfrutas de tu trabajo*
- *Envoltorio azul = un país o lugar que quieres visitar*

¿En quién confías?

Objetivo(s): facilita un proceso de reflexión con el fin de identificar aliada/os y adversario/as de cada contexto de las participantes. Esta mapeo te ayudará a facilitar una capacitación más relevante y significativa para las participantes ya que proporcionará información para contextualizar las sesiones a sus realidades.

Módulo: Ejercicios para fortalecer la confianza

Formato: Ejercicio

Nivel de habilidades: Básico

Duración: 15 minutos

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- Planes y protocolos de seguridad en organizaciones (Planeando con anticipación)
- Planes y protocolos de seguridad digital: replicar después del taller (Planeando con anticipación)
- Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

Materiales requeridos:
- Varias hojas grandes o un rotafolio

Conducir la sesión:

1. Entrega a cada participante una hoja y plantea la siguiente consigna a modo de contexto introductorio:

Ninguna persona confía ni en todo el mundo ni en nadie.

2. Dé 5 minutos para responder las siguientes preguntas individualmente. Matiza que identifiquen si sus respuestas cambiarían según fuera en un contexto personal contra activismo/laboral.

- ¿En quién confías?
- ¿A quién le confiarías tu información?

- ¿A quién no le confiarías tu información?
- ¿Quién crees que te podría estar vigilando?
- ¿Quién no te está vigilando?

Algunas personas o adversario/as que podrían surgir son: actores gubernamentales (ej. fuerzas de seguridad del Estado), empresas privadas (ej. Facebook o Google), proveedores de servicio de Internet, parejas y amistades, compañero/as.

3. Divide las participantes en grupos de 3 o 4 (máximo) para discutir sus respuestas entre ellas durante 10 minutos. Después los grupos pondrán en común.

4. Puedes dar un cierre al ejercicio explicando que, a lo largo de la capacitación, con base a las personas adversarias que identificaron en los grupos, harás énfasis en determinadas prácticas y herramientas que sean más relevantes en estos contextos.

Repensar nuestra relación con las tecnologías

Las herramientas y tecnologías no tienen poderes mágicos sobre nosotras. Nosotras decidimos qué acceso les damos.

Impresiones personales sobre la seguridad

Objetivo(s): introducir el concepto de seguridad holística; identificar nuestras motivaciones, resistencias, barreras y nociones preconcebidas en torno a la seguridad digital, género y tecnologías; explorar nuestro entendido de "seguridad".

Módulo: Repensar nuestra relación con las tecnologías

Formato: Sesión

Nivel de habilidades: Básico

Duración: 90 minutos

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- ¿En quién confías? (Ejercicio para fortalecer la confianza)
- Nuestros derechos, nuestra tecnología (Repensar nuestra relación con las tecnologías)
- Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

Materiales requeridos:
- Hojas A4 (varias por participante)
- Diapositivas (con los puntos clave descritos a continuación)
- Computadora y proyector configurados
- Rotafolio/papelógrafos

Conducir la sesión:

Parte 1 - ¿Qué es la seguridad para ti? ¿Qué es la seguridad para ti?

1. Divide las participantes en grupos pequeños de 3 o 4 (máximo). Tienen 15 minutos para discutir las siguientes preguntas entre ellas:
- ¿Qué es la seguridad para ti?
- ¿Qué te hace sentir segura?

- ¿En qué ámbitos crees que aplican estos conceptos?
  Toma en cuenta que en algunos idiomas no existen los términos equivalentes al inglés "safety" y "security" o puede haber solo una palabra para referirse a ambas, como en el caso del español: "seguridad"

2. Presenta el abordaje holístico de la seguridad en una presentación proyectada en la pared o en papeles grandes. Presta atención en explicar la importancia de la **seguridad digital, el auto-cuidado y la seguridad física en el proceso holístico** (puedes basarte en el siguiente gráfico a modo de ilustración)

3. En muchos casos, puedes estar trabajando con participantes que están tomando la capacitación para implementar medidas en sus propias organizaciones; por lo tanto, es importante explicar al grupo que este proceso estará abordando la seguridad a un nivel individual y colectivo. Las organizaciones y colectivos se componen de individuos. Para abordar la seguridad de una manera holística, necesitamos primero mirarnos a nosotras mismas, después las redes y roles que ocupamos dentro de los grupos en los que participamos y, finalmente, a nivel general de las organizaciones y colectivos.

Parte 2 - ¿Qué es la seguridad para ti?

4. Pídele a las participantes que reflexionen sobre qué significa la seguridad digital para ellas y que lo anoten en varias frases. Antes de iniciar el ejercicio, aclara que según las circunstancias - experiencias personales, prioridades, activismos, país de origen, restricciones legales -, sus conceptos pueden variar y también entre las participantes. Puedes arrancar compartiendo tu definición personal para que tengan una referencia.
5. Invítalas, sin presionarlas, a compartir lo que escribieron.

6. Una vez que varias participantes se hayan ofrecido en hablar, destaca puntos clave de lo compartido - explica que, ante todo (y especialmente en cuanto a las herramientas y tecnologías comentadas anteriormente), la seguridad digital es sobre nosotras como personas: nuestros hábitos, dispositivos, el software que utilizamos, las redes y grupos de los que formamos parte, el contexto en el que vivimos, la información que generamos y dónde la guardamos.

Parte 3 - Identificar motivaciones, resistencias y barreras

7. En grupos de 3-4 personas (máximo), las participantes discutirán sus motivaciones, preocupaciones y obstáculos relacionados con la seguridad digital, con la ayuda de las siguientes preguntas:

- ¿Por qué quieren aprender más sobre seguridad digital?
- ¿Cuáles son sus motivos personales en participar en este taller?
- ¿Cuáles son sus expectativas?
- ¿Consideran que tienen resistencias personales ante la seguridad digital?
- ¿Qué retos han enfrentando a la hora de aprender sobre seguridad digital? O, ¿qué identifican que les impidió aprender en el pasado?

8. Cada grupo comparte sus reflexiones y discusiones a las demás. Este es un momento crítico para la facilitación: para adaptar las sesiones con el fin de que sean realmente relevantes a los contextos de las participantes, es extremadamente importante que prestes atención a las motivaciones, resistencias y obstáculos compartidos en el grupo.

Parte 4 – Seguridad digital, género y mitos en torno a las tecnologías

9. Prepara, desde antes, información sobre los siguientes ejemplos de mitos y conceptos errados sobre la seguridad digital, el género y las tecnologías. Aparte de basar tu explicación en tu experiencia y conocimientos, asegúrate de encontrar maneras de relacionar la discusión con algunas de las motivaciones, resistencias y obstáculos identificadas por las participantes en la actividad anterior:

"La seguridad digital es difícil."
La seguridad digital es un proceso. Conforme aprendas más, más probable es encontrar prácticas inseguras; ***¡no te estreses!*** *No sientes que tienes que cambiar todos tus hábitos en un solo día (o en un solo taller) ¡Es un paso positivo y sano que estés empezando este camino!*

Cuanto más avances, más te darás cuenta que, casi nunca, existe una sola respuesta para las preguntas que van emergiendo sobre seguridad digital. Lo más importante es reconocer que tú te conoces mejor que nadie (o nada); así que tú eres la que sabe cuáles son los cambios y nuevos hábitos que puedes ir introduciendo en tu día a día. Es mejor empezar con algo que sientas que puedas implementar de manera realista, en vez de poner el listón muy alto y desanimarte.

"La seguridad digital consiste en aprender sobre herramientas nuevas que ninguna amiga o compañero/a utiliza"

En realidad, la mayoría de las prácticas básicas pilares no están relacionadas con una herramienta en sí. Cambiar regularmente tus contraseñas, revisar las configuraciones de privacidad de tus cuentas, proteger tus dispositivos con contraseñas, respaldar frecuentemente tus datos... tiene mucho más que ver con tus hábitos y comportamiento que con una herramienta en concreto.
El proceso de seguridad digital que estamos empezando aquí consiste en brindarte información sobre qué necesitas para que puedas tomar decisiones con fundamento sobre tu seguridad digital. Está enfocado en aprender más sobre las plataformas que usas, las implicaciones que tiene en nuestra vida y trabajo escoger ciertas herramientas o prácticas; y mejorar las maneras en que utilizamos las tecnologías en nuestro cotidiano.

Juntas trabajaremos para mejorar estas prácticas conforme vamos aprendiendo más sobre los riesgos que enfrentamos cuando tomamos estas decisiones y cambios. Aprenderemos y compartiremos información entre nosotras que pueda ayudarnos a tomar mejores decisiones sobre qué prácticas necesitamos cambiar y, lo que también es importante destacar, las que ya hacemos bien. Y sobre todo, tú tienes la última palabra: ¡la decisión es tuya!

"Las herramientas de seguridad digital son caras."

*En realidad, la mayoría de las herramientas digitales **son gratuitas.** La cantidad y variedad de herramientas disponibles incrementa cada día. Los proyectos FLOSS (Free Libre and Open Source Software: Software Gratuito, Libre y de Código Abierto) están constantemente creando herramientas gratuitas que funcionan en muchos sistemas operativos, tanto en computadoras como en dispositivos móviles. Además, muchas de las plataformas web más conocidas han implementado características de seguridad.*

"¡No sé nada sobre la seguridad digital!"

Te sorprenderías si supieras que la mayoría de nosotras ya le hemos dado vuelta a nuestras propias prácticas sin darnos cuenta. Por ejemplo, muchas utilizan contraseñas para proteger sus dispositivos (computadoras y celulares) y utilizan seudónimos/identidades separadas para su trabajo y su vida privada; algunas ya utilizan diferentes apps o herramientas para comunicarse con ciertas personas sobre determinados temas.

Opcional: para este mito en concreto, puede ser buena idea dedicar unos minutos a preguntarle a las participantes sobre prácticas de seguridad digital que ya llevan a cabo. Anótalas en un papel y cuélgalo en un lugar visible para que sirva de referencia a lo largo de la capacitación.

"No utilizo (o apenas utilizo) Internet, así que la seguridad digital no importa"
La seguridad digital no sólo tiene que ver con lo que haces online. Prácticas offline como consultar información (contactos, imágenes, documentos, vídeos, audios, etc.) que tienes almacenada en tu computadora, celular y USBs; además de tomar conciencia de dónde están tus dispositivos o quién tiene acceso a ellos es fundamental. Es especialmente importante saber qué apps y programas (software) están instaladas en nuestros dispositivos. A veces, para acceder ciertos tipos de información en nuestros dispositivos, tenemos que instalar nuevas apps o crear nuevas cuentas sin darnos cuenta.

"No tengo nada que esconder y aunque fuera así, no importa porque el gobierno (o quien sea) lo va a averiguar de todas maneras"

Explicado en el proyecto de Tactical Tech 'Yo y Mi Sombra' [1]:

La privacidad no tiene que ver con esconder sino con el anonimato, el poder y control; es sobre tu habilidad en decidir cómo te presentas en el mundo.

Puedes pensar que no tienes nada que esconder, pero párate un momento a pensar qué tipos de información compartes: ¿con quiénes te comunicas? ¿En qué canales/medios? ¿Son públicos o abiertos?

De alguna manera u otra, todos los días tomamos decisiones sobre los tipos de información que compartimos y con quiénes la compartimos. También necesitas tomar en cuenta que, aunque no tengas nada que esconder, puede ser que en el futuro sí. ¡Seguramente querrás prepararte para esa posibilidad!

¿Alguna vez te has sentido desbordada o abatida al enterarte sobre la vigilancia digital, las tácticas de acoso de los gobiernos o de otros grupos contra las defensoras de derechos humanos? Dentro de nuestros activismos, es normal atravesar estos momentos y no sólo en el contexto de seguridad digital o amenazas online. Aquí es donde comienza este proceso holístico. Juntas, construiremos un abordaje de múltiples capas que nos ayude a protegernos y nuestra información.

Parte 5 – Afirmaciones para cerrar

10. Dé un cierre a la actividad sugiriendo algunas (o todas) las siguientes ideas y alientos para el grupo. De nuevo, considera las motivaciones, resistencias y obstáculos identificadas por las participantes

- ¿Cómo podemos superar el obstáculo de pensar "*la tecnología y yo no nos llevamos bien*"?

    - ¡Las herramientas y la tecnología no tienen poderes mágicos sobre nosotras! Nosotras somos quienes decidimos cuándo accedemos a ellas y, si algo ocurre, podemos empezar de vuelta o cambiar las herramientas que usamos.

    - Solamente nosotras sabemos qué prácticas de seguridad digital son las más apropiadas para nosotras para implementar en nuestras vidas.

Opcional: *si tu capacitación va a incluir específicamente este resultado deseado, es un momento muy oportuno para explicar a las participantes que, conforme van avanzado juntas en el proceso formativo, escribirán sus propios planes y estrategias sobre las prácticas y herramientas que van a implementar. Estos planes incluirán metas personales que las animarán a avanzar a su propio ritmo.*

Referencias:

- https://myshadow.org/es/tracking-so-what
- https://ssd.eff.org/es/module/siete-pasos-para-la-seguridad-digital

Nuestros derechos, nuestra tecnología

Objetivo(s): discutir sobre la relación entre derechos y tecnologías, ayudar a identificar amenazas actuales en sus derechos e introducir conceptos básicos y relevantes sobre seguridad digital.

Módulo: Repensar nuestra relación con las tecnologías

Formato: Sesión

Nivel de habilidades: Básico

Duración: 50 minutos

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)
- ¿En quién confías? (Ejercicio para fortalecer la confianza)
- Introducción al cifrado (Cifrado)
- Anonimato (Anonimato)
- Privacidad (Privacidad)
- ¿Cómo funciona Internet? (Principios básicos de seguridad digital)
- Una Internet Feminista (Violencia en línea contra mujeres)

Materiales requeridos:
- Rotafolio o papelógrafos
- Marcadores de colores
- Copias de reportajes y noticias sobre derechos digitales contextualizados en los países/regiones de origen de las participantes (una copia para cada 3-4 participantes)

Recomendaciones:
- La sección de referencias de esta sesión incluye enlaces a organizaciones que publican regularmente noticias sobre derechos digitales. Asegúrate que los contenidos cubran un espectro de temáticas relacionadas con derechos digitales como la vigilancia, cortes de Internet, censura de contenidos y otros ejemplos de amenazas comunes en dichos contextos.

Conducir la sesión:

Parte 1 – Conectando derechos con tecnología

1. Divide las participantes en grupos de 3-4 (máximo) y entrega a cada grupo 1 ó 2 hojas grandes de papel y marcadores. Cada grupo tiene 10 minutos para hacer una lista de derechos humanos. Cómo cada grupo define este concepto es cosa suya. Anotarán todo en los papeles grandes entregados.

2. Cada grupo echa un vistazo a su lista. Discuten, durante 10 minutos, cómo estos derechos humanos se relacionan con la tecnología (por ej, "qué impacto tiene la tecnología sobre los derechos humanos") Puedes dar un ejemplo trazando conexiones entre tecnologías y derechos humanos en el papelógrafo de uno de los grupos. Pueden anotar las relaciones en otro papel si quieren.

3. Ahora comparte con cada grupo una selección (preparadas desde antes) de reportajes y noticias sobre derechos digitales (véase "materiales requeridos") Los grupos tienen 15 minutos para leer los contenidos por encima y hacer una lluvia de ideas de las amenazas digitales/online contra los derechos humanos (que enlistaron anteriormente) que implican las noticias que leyeron. Matiza que los contenidos que entregaste son solo a modo de guía. Si conocen otros casos o amenazas, pueden incluirlas también.

4. Cada grupo presenta brevemente lo que trabajaron.

5. Se abre una discusión entre todas sobre cómo pueden las defensoras sentirse fácilmente desbordadas o indefensas cuando se enfrentan a los distintos riesgos y amenazas que emergen online. Si ya tuvieron esta conversación en la sesión de "Impresiones personales sobre la seguridad" de este módulo, puedes simplemente hacer referencia a lo que hablaron.

6. Procura dejar suficiente tiempo (15-20 minutos) para cerrar esta parte de la sesión, ofreciendo ejemplos de prácticas o herramientas disponibles para estas amenazas. Si ya hiciste esto en la sesión de "Impresiones personales sobre la seguridad", toma en cuenta, a la hora de dar recomendaciones, las motivaciones, resistencias y obstáculos identificadas.

Parte 2 –Seguridad digital y conceptos de seguridad digital

7. Ahora que ya cubrieron prácticas y herramientas básicas de seguridad digital en respuesta a las amenazas online/digital contra los derechos humanos discutidos en la Parte 1, presenta ahora algunos conceptos clave de seguridad digital con implicaciones concretas en los derechos de **anonimato, privacidad y cifrado.** En algunos contextos, quizás sea importante también incluir la **circunvención** como un ejemplo.

8. Subraya la importancia de que están dando un paso crítico hacia abordar su propia seguridad digital dentro de este taller y que empezarán el proceso de aprender cómo contrarrestar algunas de las amenazas que atentan contra ellas.

Si ya cubriste la sesión de "Impresiones personales sobre la seguridad" de este módulo, vuelve a poner sobre la mesa algunas de las impresiones y definiciones de seguridad digital que las participantes compartieron en los pasos 2, 3 y 4 de la sesión.

Si aún no llegaron a esta sesión, será buena idea discutir con las participantes qué significa la seguridad digital en un sentido más amplio, con base en tu experiencia como facilitadora.

9. Invita a las participantes a compartir sus propias definiciones de qué significa la privacidad para ellas y cómo se sienten con respecto al estado actual de privacidad en la era digital. A continuación, explica qué es la privacidad digital/online. Conforme vayas presentando, asegúrate de encontrar maneras de animar activamente a las participantes a reclamar su derecho a la privacidad.

10. Repite el paso 9, pero esta vez aborda el concepto de anonimato: qué significa para ellas y cómo se sienten en la actualidad con respecto a este tema. Resuelve posibles dudas utilizando ejemplos. De nuevo, toma en cuenta de generar un clima de agencia con respecto a sus derechos y deja claro las diferencias entre privacidad y anonimato como dos conceptos distintos.

11. Presenta el concepto de cifrado y explícales que irán aprendiendo sobre ello a lo largo de la capacitación a través de diferentes prácticas y herramientas. Repasa algunas de estas prácticas y herramientas. Dibuja conexiones entre ellas y las discusiones anteriores en torno a los derechos digitales, la privacidad y el anonimato.

10. A modo de cierre, sugiere algunas organizaciones que brindan apoyo y hacen injerencia política en los derechos digitales dentro los contextos geográficos de las participantes para que después puedan investigar y adquirir una familiaridad por su cuenta. Por ejemplo, si estás trabajando con un grupo de Latinoamérica, organizaciones como Derechos Digitales, R3D, Global Voices, Karisma y Access Now.

Referencias:

- https://www.derechosdigitales.org
- https://r3d.mx
- https://karisma.org.co
- http://acceso.or.cr
- https://articulo19.org

Her-Story (las historias de las mujeres) en las tecnologías

Objetivo(s): brindar una mirada empoderada del liderazgo de las mujeres a lo largo de la historia y dentro de la evolución de la tecnología moderna, con el objetivo de desmontar estereotipos y constructos de género perjuiciosos.

Módulo: Repensar nuestra relación con las tecnologías

Formato: Sesión

Nivel de habilidades: Básico

Duración: 20 minutos

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- Una Internet Feminista (Violencia en línea contra mujeres)
- Aquelarre de Brujas (Ejercicios de cierre y evaluación)

Materiales requeridos:
- Fotos de diferentes mujeres en la tecnología (con nombres)
- Biografía de cada mujer (como referencia para la facilitadora)
- Un trozo de cuerda (aprox. 1 metro)
- Pinzas (1 o 2 para cada foto)

Recomendaciones:
- El siguiente documento es un recurso nutrido de historias de mujeres para esta sesión (en español): http://www.rebelion.org/docs/141550.pdf

Conducir la sesión:

1. Presenta esta sesión como un ejercicio para desarrollar una memoria colectiva que reconozca las mujeres dentro de las tecnologías a lo lo largo de la historia (las her-stories: las historias de mujeres) Pregunta al grupo:

> *¿Cuántas veces has escuchado que las mujeres y la tecnología son agua y aceite?*
>
> *¿Cuántas veces has escuchado que nuestro lugar es estar fuera de vista y no en el ámbito público o académico?*

2. El grupo se sienta en círculo (en el suelo o sentadas en las sillas). Introduce el tema de las brechas de género en las tecnologías: qué es, qué sabemos sobre este tema.
3. Invita a las participantes a compartir sus propias historias sobre fortalezas y resistencias en la tecnología. Puedes arrancar con la consigna: ¿qué es la tecnología para ti? ¿Es algo bueno o malo? Como ejemplo, comparte tu propia historia sobre la tecnología para animar a las participantes a sentirse más abiertas y cómodas.

4. Ahora es el turno de las participantes. Las que quieran, comparten sus anécdotas. Después, muestra las fotos de algunas mujeres que han participado activamente en la historia de las tecnologías y preséntalas. Coloca las fotos y biografías en la mesa o en el suelo sin orden específico. Pregunta: ¿quién crees que empezó en el mundo de las tecnologías?

5. Cuelga las fotos en la cuerda y pide a las participantes ordenarlas cronológicamente (por fecha de nacimiento o por fecha de logros) basándose en las biografías. Estamos creando una línea de tiempo de mujeres en la tecnología.

6. Repasa la línea de tiempo. ¿Cuántas mujeres conocían ya? ¿Cuáles son totalmente nuevas para ellas? Deja la línea de tiempo ahí visible en la sala durante el resto del taller. Al terminar la sesión, invita al grupo a acercarse a leer más en detalle sobre estas increíbles mujeres.

Opcional: *como la línea de tiempo va a estar visible durante todo el taller, otra manera de conducir esta sesión es cerrando el ejercicio una vez que el grupo haya repasado toda la línea de tiempo. Una vez que todas estén sentadas de nuevo, puedes compartir la biografía de la primer mujer de la línea de tiempo y hablar de la relevancia de su contribución.*

Al comenzar cada día del taller (según la duración y el número de participantes), invita a 1 ó 2 participantes a hacer lo mismo con 1 ó 2 mujeres de la genealogía para que, al final del taller, cada participante haya tenido la oportunidad de conducir una mini-sesión compartiendo las historias de las mujeres en las tecnologías.

Referencias:

- **https://vimeo.com/lelacoders**
- **http://donestech.net/es**

Principios básicos de seguridad digital | Parte 1

Desde cómo funciona Internet y técnicas de navegación más seguras, hasta cómo proteger dispositivos contra malware y acceso sin consentimiento... y mucho más.

¿Cómo funciona Internet?

Esta sesión fue desarrollado conjuntamente con Mariel García (SocialTIC) y Spyros Monastiriotis (Tactical Technology Collective)

Objetivo(s): compartir una comprensión de los flujos de información de Internet, las distintas vulnerabilidades que emergen y buenas prácticas de seguridad relacionadas a cada componente y tramo de la cadena.

Módulo: Principios básicos de seguridad digital | Parte 1

Formato: Sesión

Nivel de habilidades: Básico

Duración: 1 hour

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- ¿En quién confías? (Ejercicio para fortalecer la confianza)
- Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)
- Tus derechos, tu tecnología (Repensar nuestra relación con las tecnologías)

Materiales requeridos:
- *¿Cómo funciona Internet?* Tarjetas de representaciones icónicas de los distintos componentes de la ruta que sigue un correo electrónico desde que se envía hasta que es recibido:
    - Dispositivos (computadora/celular) (x 2)*
    - Módem (x2)
    - Poste telefónico/Fibra óptica subterránea (x 2)
    - Proveedor de servicio de Internet (x 2)
    - Servidores Google (x 1)
    - Simulacro de email (x 2, o más)

  *Representa la computadora y el celular en la misma tarjeta para evitar confusiones

- Documentos con sugerencias sobre prácticas de seguridad digital
- Papel para utilizar a modo de pizarrón: un trozo de 4 metros y dos trozos de 1 metro cada uno.
- Marcadores de colores
- Cinta adhesiva

- Diapositivas (con puntos clave comentados a continuación)
- Computadora y proyector ya configurados
- Altavoces/bocinas

Recomendaciones:

- Procura cubrir todas las preguntas que puedan surgir. Es importante cerrar la sesión cubriendo las inquietudes que puedan surgir en torno a las vulnerabilidades comentadas en la sesión y que sientan que tienen la información necesaria para tomar medidas. Evita crear un entorno de miedo, estrés o ansiedad - brinda suficiente información y recursos, además de señalar otras oportunidades para formación (si es posible).

Conducir la sesión:

Parte 1 - Cómo funciona Internet – Flujos de información y puntos de vulnerabilidad.

1. Esta parte del taller comenzará a modo de juego. Cada participante recibe tarjetas representando diferentes componentes de una cadena de flujo de información (módem, computadora, edificio de proveedor de servicio de internet, etc.). Pide a las participantes que las ordenen correctamente para mostrar cómo se envía un correo a través de Internet.

2. Haz observaciones del orden de las tarjetas y repasa el proceso con el grupo. Pide a una persona voluntaria que explique el proceso de nuevo en sus propias palabras. Recomendamos pedir que tres personas en total cuenten el proceso de vuelta. Puedes cambiar las ilustraciones de referencia y en qué orden se explica para darle más variedad al ejercicio. Procura un tiempo para resolver dudas también.

3. Puedes apoyarte en un recurso audiovisual como (https://www.youtube.com/watch?v=7_LPdttKXPc) para ayudar a las participantes a identificar si están ordenadas correctamente las tarjetas.

Opcional: *para grupos más grandes, en vez de una tarjeta por persona, reparte una por pareja; para grupos más pequeños, coloca todas las tarjetas en el suelo y debate en grupo el orden.*

Parte 2 - Vulnerabilidades

4. Una vez completado el paso anterior, las participantes colocan cada tarjeta en un papel grande en el suelo. Repasa de nuevo la cadena, esta vez señalando y explicando las vulnerabilidades en cada etapa (comparte brevemente algunas buenas prácticas relevantes para generar una sensación de calma y confianza entre las participantes)

Comentaremos algunas vulnerabilidades a continuación. Puedes agregar otras prácticas o vulnerabilidades que consideres relevantes a tu propio contexto o los contextos de las participantes. También puedes compartir algunos ejemplos de prácticas de otros colectivos con los que trabajas, con el fin de ayudar a las participantes pensar cuáles podrían ser prácticas buenas o malas en su caso.

Dispositivo 1 (computadora/celular): inseguridad física; pérdida de información

Módem 1: sniffing de WiFi; información sin cifrar
Poste telefónico/fibra óptica subterránea: no aplica

Proveedor de servicio de internet: solicitudes de datos y metadatos de instancias gubernamentales locales/nacionales

Servidores de Google: vigilancia internacional; contraseñas inseguras y phishing, solicitudes de instancias gubernamentales nacionales

Poste telefónico/fibra óptica subterránea 2: N/A

Módem 2: problemas de seguridad al utilizar las conexiones de terceros (ej. cibercafé)

Dispositivo 2: software malicioso; borrado inseguro de datos

Parte 3 - Buenas prácticas de seguridad digital
5. Una vez que se hayan centrado en las vulnerabilidades, para que no sea demasiada información para las participantes que tienen menos experiencia en estos temas, cada grupo tomará un papel que describa una posible solución. Este papel será el detonante para discutir en grupo.

Al final, los grupos tendrán entre 30 segundos y un minuto para presentar sus ideas (una de las facilitadoras tomará notas y aportará retroalimentación). Las facilitadoras se moverán por el espacio dando explicaciones cortas y respondiendo preguntas y, sobre todo, alentando la discusión entre las participantes.

Es importante que, conforme avance esta actividad, las facilitadoras expliquen los conceptos básicos de cada solución. También, según el nivel de interacción y ritmo del taller, quizás no dé para cubrir todas las propuestas.

Algunas de las más importantes para tomar en consideración son:

Inseguridad física: reduce la exposición de los dispositivos de tu organización a personas desconocidas.

Inseguridad física: utiliza bloqueos de dispositivos en tu oficina y casa.

Pérdida de información: guarda tu respaldo en un lugar que no sea tu oficina o casa.

Pérdida de información: escoge una persona para encargarse de los respaldos en tu organización.

Intevención de redes (WiFi sniffing): retira todas las indicaciones que muestren la contraseña de WiFi.

Intervención de redes (WiFi sniffing): cambia la contraseña de tu WiFi frecuentemente.

Datos sin cifrar: asómate a una criptofiesta en tu ciudad o participa en un taller.
Datos sin cifrar: lee la sección sobre cifrado del manual "Security in a Box".

Solicitudes de datos y metadatos por parte de entidades gubernamentales locales/nacionales: trabaja con organizaciones de derechos digitales para encontrar maneras para protegerte legalmente.

Solicitudes de datos y metadatos por parte de entidades gubernamentales locales/nacionales: investiga qué dicen las leyes en tu país sobre la intervención de comunicaciones.

Vigilancia internacional: cámbiate a servicios seguros para realizar búsquedas, administrar tu correo, alojar tus datos y comunicaciones en general.

Contraseñas inseguras: utiliza contraseñas largas y complejas.

Contraseñas inseguras: utiliza KeePass para recordar todas las contraseñas que tienes.

Phishing: piensa antes de hacer clic (presta atención donde introduces tus datos de acceso a una cuenta).

Utilizar el WiFi de otras personas: siempre cierra adecuadamente tu sesión.
.
Utilizar el WiFi de otras personas: cuéntanos -¿qué no deberías estar revisando cuando estás en el WiFi de otra persona?

Software malicioso: instala un programa de antivirus y ejecútalo manualmente cada semana.

Borrar datos de manera segura: usa Cmd+derecha para vaciar la papelera en Mac.

Borrar datos de manera segura: utiliza programas como Eraser o CCleaner.

Parte 4 - Asuntos y recursos pendientes
6. Este momento de la sesión es para sondear preguntas relacionadas con seguridad digital que no hayan surgido en el taller hasta ahora, además de discutir temas relevantes en las comunidades de las participantes. Aprovecha para compartir materiales para seguir aprendiendo y mantenerse al día. La facilitadora hará ronda de preguntas, dará unas pistas de posibles respuestas y mencionará referencias que pueden servir para responderlas más en profundidad.

Referencias:

- https://securityinabox.org/es
- https://ssd.eff.org/es
- https://myshadow.org/es
- http://www.sinmiedo.com.co
- https://cuidatuinfo.org
- https://temboinalinha.org
- https://prism-break.org/es

Creando contraseñas más seguras

Esta sesión está basada en el módulo "Prácticas de contraseñas más seguras", desarrollado por Cheekay Cinco, Carol Waters y Megan DeBolis para LevelUp.

Objetivo(s): revisar vulneración de contraseñas - cómo son comprometidas, cuáles son las implicaciones-, cómo crear contraseñas más robustas y desarrollar mejores hábitos en relación con nuestras contraseñas.

Módulo: Principios básicos de seguridad digital | Parte 1

Duración: 45 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- ¿Cómo funciona Internet? (Principios básicos de seguridad digital | Parte 1)
- Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

Materiales requeridos:
- Proyector
- Diapositivas
- Papel
- Conexión a Internet/WiFi para descargar KeePass

Conducir la sesión:

Parte 1 - Introducción

1. Comienza preguntando a las participantes:
   - ¿Cuándo fue la última vez que cambiaste alguna de tus contraseñas?
   - ¿Tienes contraseñas diferentes para cada cuenta?
   - ¿Anotaste tu contraseña en alguna parte como un post-it?
   - ¿Almacenas todas tus contraseñas en un documento sin cifrar?

- ¿Tus contraseñas están en tu celular?

Parte 2 - Por qué las contraseñas son importantes

2. Antes de empezar a hablar de la importancia de las contraseñas, pide a las participantes enumerar toda la información que es asegurada con una contraseña. ¿Qué información tienen en sus cuentas de correo, cuentas de redes sociales y celulares? ¿Qué pasaría si otra persona pudiera acceder a esta información?

3. Ahora, comparte algunas razones por las que las contraseñas son importantes:

- Las contraseñas brindan acceso a un abanico de cuentas importantes como tu correo, cuentas bancarias, redes sociales, etc.
- Estas cuentas suelen contener información muy sensible y nos permiten ser "nosotras mismas" en interacción orgánica con las demás a través de diferentes servicios digitales: enviar un mensaje a través de una plataforma de red social, enviar un correo, realizar una compra online, etc.
- También pueden darnos la oportunidad de asumir otras identidades - cualquier persona que accede a una contraseña de una cuenta puede, en efecto, simular ser la propietaria de la cuenta.
- Las contraseñas también dan acceso a otras cosas - puntos de acceso Wi-Fi, desbloquear celulares, iniciar sesión en computadoras, descifrar dispositivos, archivos y mucho más.

Parte 3 - ¿Qué pasa si comprometen tu contraseña?

4. Comparte papeles con las participantes y pídeles hacer una lista de todas las plataformas donde se acuerden que tienen cuentas. Después, que anoten qué pasaría si alguien tuviera su contraseña y pudiera acceder a sus cuentas o dispositivos.

- Pueden robar (copiar) o borrar información importante o archivos; si esto sucede, quizás no te des cuenta de ello inmediatamente. Podría ser desde documentos y archivos con información confidencial, hasta contactos del directorio y correos electrónicos.
- Podrían robar o malversar fondos a través del acceso de tarjetas de crédito o cuentas bancarias.
- Pueden usar cuentas de correo o plataformas de redes sociales para enviar spam o hacerse pasar por ti o tus amigo/as, familiares y compañero/as.
- O secuestrar tu cuenta a cambio de un "rescate" que podría ser dinero, acceso a contactos.
- Alguien indebido con una contraseña podría acceder y revisar tus comunicaciones y actividades sin tu conocimiento.
- A través del acceso de una cuenta de correo, se podría desencadenar un "efecto dominó" y restablecer las contraseñas de otras cuentas a través de links de solicitud, hasta dejar a la persona legítima fuera de todas de sus cuentas.

Parte 4- ¿Cómo son las maneras más comunes de comprometer una contraseña?

5. Comparte algunas prácticas que pueden resultar en que otras personas tengan acceso a tus contraseñas:

- Cuando las compartes con otras personas o las almacenas en lugares fáciles de descubrir, por ejemplo, en un post-it pegado cerca de la computadora.
- Cuando alguien te ve escribiendo una contraseña en tu pantalla y lo anota o se acuerda de ella.
- Si estás usando un cliente de correo que no utiliza SSL (https) durante toda la sesión (y no sólo en el login), las contraseñas y demás información queda potencialmente expuesta a cualquiera que tenga acceso a tu conexión.
- Al acceder físicamente a un dispositivo, se puede obtener las contraseñas a través de la configuración "Save My Password" ("Guarda mi contraseña") o "Remember Me" ("Recuérdame") de tu navegador. Esto es aún más probable si el disco de tu dispositivo no está cifrado.
- Malware, como los keylogger (registrador de teclas), puede registrar cada golpe de tecla de un dispositivo y enviarlo a un tercero, revelando no sólo contraseñas sino potencialmente una cantidad mucho más amplia de información confidencial.
- Las brechas de seguridad de una plataforma también pueden exponer información sobre sus usuarias.

Parte 5 - ¿Cómo podemos crear contraseñas más robustas?

6. Explica que si utilizan la misma contraseña para todo y esa contraseña es comprometida, todas las cuentas podrán ser vulneradas. Comenta algunas características para contraseñas más seguras y robustas:

- **Duración:** en pocas palabras, ¡cuanto más larga, mejor! 12 caracteres es el mínimo recomendable para contraseñas robustas y 20 es mejor todavía.

- **Complejidad:** utiliza una contraseña alfanumérica, con mayúsculas y minúsculas, una mezcla generosa de números y caracteres especiales.

- **Cambios frecuentes:** cambia a menudo tus contraseñas, particularmente las de tus cuentas más confidenciales y, sobre todo, cámbialas si recibes un correo legítimo y verificado (no phishing) diciéndote que la cuenta de determinado servicio ha sido comprometida.

Utilizar **frases enteras** -imagina varias contraseñas juntas en una misma 'frase'- es un ejemplo de práctica segura de contraseñas. Aquí van unos ejemplos:

- **NoALaMineriaEnAmericaLatina**

- **AbortoSiAbortoNoEsoLoDecidoYo**

- N**osotrxsNoCruzamosFronterasEllasNosCruzanANosotrxs**

7. Propón a las participantes dedicar varios minutos a crear algunos ejemplos de contraseñas robustas. Recuérdales que tengan en cuenta la importancia de la confidencialidad de la información que están resguardando a la hora de escoger la longitud y complejidad de sus contraseñas - quizás quieran utilizar contraseñas más robustas para sus cuentas más importantes y unas menos complejas (pero aún seguras) para sus cuentas sin tanta relevancia.

Referencias:

- https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras
- https://securityinabox.org/es/guide/passwords

Malware & Virus

Objetivo(s): abordar, en un contexto de riesgos cercano a las realidades de las defensoras, conceptos básicos de malware y la exposición de nuestros dispositivos a distintos tipos de malware y software malicioso.

Módulo: Principios básicos de seguridad digital | Parte 1

Duración: 30 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- ¿Cómo funciona Internet? (Principios básicos de seguridad digital | Parte 1)
- Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)
- ¡Empecemos de nuevo! (Principios básicos de seguridad digital | Parte 2)

Materiales requeridos:
- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados

Recomendaciones:
- Idealmente, después de esta sesión, sigan con la de "Cómo hacer más segura tu computadora", también incluida en este módulo.

Conducir la sesión:

Parte 1 - Introducción al Malware

1. Explica a las participantes qué es el malware, un repaso de algunos tipos - como mínimo, recomendamos cubrir los siguientes:
- Troyanos
- Spyware
- Ransomware

- Keylogger (registrador de teclas)
- Virus

El ransomware y los registradores de teclado (keyloggers) son tipos de malware cada vez más comunes en el contexto de las defensoras en Latinoamérica; si estás trabajando con un grupo de mujeres en esta región, será especialmente importante abordarlas. En general, asegúrate de incluir estudios de caso y ejemplos de malware que sean comunes en las realidades de las participantes de tu taller.

Parte 2 - ¿Cómo te puedes infectar?

2. Explica algunas de las maneras más comunes de infección de malware. También es importante explicar los distintos propósitos o motivaciones que puede tener el uso de malware:

- Algunos se viralizan a una escala amplia sin ningún objetivo concreto.
- Otros van dirigidos específicamente a activistas, periodistas o disidentes para obtener acceso a sus datos y comunicaciones.
- O a personas que están en contacto con una red de activistas y defensoras y que, a través de infectar su equipo, alcancen el resto de su red.

Parte 3 - Comparte ejemplos que afecten a mujeres y defensoras de derechos humanos

3. Concluye la sesión compartiendo ejemplos de casos de infección de malware comunes en el contexto de mujeres y defensoras; puedes basarte en estudios de caso (de blogs, portales de noticias o desde la experiencia personal de cada una). Recuerda anonimizar las fuentes al menos que tengas permiso explícito de la(s) persona(s) afectada(s). Aquí mostramos algunos ejemplos de casos. Quizás conozcas casos similares más relevantes a tu contexto.

- Una mujer que recibió un correo que oferta boletos gratuitos a un concierto; el enlace que contenía el correo infectó su smartphone (celular inteligente) con malware.

- Una activista recibió un correo de quien era, aparentemente, un/a compañero/a; al hacer clic en el enlace del correo, un mensaje aparece diciendo que su disco duro está cifrado y que necesita pagar para obtener acceso de vuelta a sus datos.

Referencias:

- https://securityinabox.org/es/guide/malware/
- https://ssd.eff.org/es/module/protegi%C3%A9ndote-contra-el-malware

Navegación segura

Objetivo(s): brindar una introducción sobre prácticas de navegación web segura, incluyendo un repaso a plugins y otros servicios que pueden utilizarse para crear un entorno de navegación más seguro.

Módulo: Principios básicos de seguridad digital | Parte 1

Duración: 45 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Ejercicios/sesiones relacionadas:
- ¿Cómo funciona Internet? (Principios básicos de seguridad digital | Parte 1)
- Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

Materiales requeridos:
- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Conexión WiFi

Conducir la sesión:

Parte 1 - Escoger un navegador
1. Arranca la sesión preguntando a las participantes qué navegadores web utilizan y qué otras conocen. Presenta **Firefox** - explica los beneficios de utilizarlo y comenta brevemente las diferencias que existen con otros navegadores conocidos como Google Chrome o Internet Explorer.

Opcional: *si estás trabajando con un grupo que habla español, puedes echar mano a este vídeo de Ella para detonar una discusión: https://vimeo.com/109258771*

Parte 2- Prácticas más seguras de navegación
2. Existen bastantes prácticas de navegación más segura que puedan ser compartidas y discutidas con las participantes. No tienes que repasarlas todas, pero recomendamos dar a conocer suficientes para que el grupo pueda barajar opciones (toma en cuenta el contexto de las participantes a la hora de hacer recomendaciones).

3. Subraya que aún están revisando algunas prácticas y no específicamente herramientas más allá de navegadores web. Algunas participantes estarán ya dispuestas a cambiar de navegador, mientras otras no, así que antes de discutir herramientas más específicas como complementos y plugins, es importante que aterricen la discusión.

Aquí van algunos ejemplos de prácticas que pueden discutir:

- Estar atenta a intentos de phishing;
- Bloquear anuncios integrados en sitios y anuncios emergentes;
- Cómo funcionan los cookies - asegúrate de comentar que pueden ser necesarios para que un sitio/plataforma funcione, pero que también tienen desventajas;
- Deshabilitar y borrar cookies de los navegadores,
- Eliminar historial de navegación;
- No guardar las contraseñas en la configuración de tu navegador;
- Comprobar las extensiones que instalas en tu navegador;
- Habilitar la opción "No rastrear" (Do Not Track) en tu navegador;
- Alternativas de buscadores a Google (como Duck Duck Go);
- ¿Quién implementa el rastreo online y por qué? (Tanto https://trackography.org/ como https://www.mozilla.org/es-MX/lightbeam/ son buenos recursos);
- Discutir HTTP vs HTTPS;
- ¿Qué es una VPN (Virtual Private Network/Red Privada Virtual) y cuándo la deberías usar?
- ¿Qué hace exactamente el modo incógnito y cuándo la deberías usar?

Parte 3 – Herramientas y extensiones para una navegación más segura

4. Presenta, ahora que abordaste algunas prácticas para una navegación más segura, determinadas herramientas - específicamente plugins para el navegador - puedan ayudar a automatizar o facilitar la adopción de algunas de las prácticas comentadas anteriormente.

5. Dé a conocer las siguientes herramientas, explicando cómo funciona cada una. Recuerda compartir los links de descarga. Es esencial que las participantes comprendan por qué cada una de las herramientas es útil y relevante; si no son explicadas de manera clara, puede dar lugar a que las participantes tomen decisiones sin fundamento sobre su privacidad y anonimato en línea.

Herramientas de navegación para computadoras:

- No Script: https://noscript.net
- Adblock Plus: https://adblockplus.org/es
- Privacidad Badger: https://www.eff.org/privacybadger
- HTTPS Everywhere: https://www.eff.org/https-everywhere
- Click & Clean: https://www.hotcleaner.com
- Tor browser: https://www.torproject.org/download/download-easy.html.en
- Disconnect: https://disconnect.me

- uMatrix: https://addons.mozilla.org/es/firefox/addon/umatrix

Herramientas de navegación para celulares:

- HTTPS Everywhere: https://www.eff.org/https-everywhere
- https://myshadow.org/resources
- Orfox: https://guardianproject.info/apps/orfox
- Orbot: https://www.torproject.org/docs/android.html.en
- Tor for iPhone: https://mike.tig.as/onionbrowser

Otras prácticas & funcionalidades

- *Modo incógnito (Modo privado*

Esta funcionalidad suele generar confusiones ya que muchas personas usuarias no la comprenden - quizás las participantes no tengan una comprensión clara de cómo funciona el modo incógnito en el navegador y cuándo puede ser útil. Explica cómo funciona el modo incógnito (y otros parecidos) y ofrece algunos ejemplos de cuándo podrían ser útiles.

- *Prácticas Wi-Fi seguras*

  En último lugar, dedica un tiempo a discutir y, si es posible, demostrar, unas cuantas prácticas básicas de seguridad cuando te conectas a una conexión Wi-Fi - esto incluye cambiar la contraseña por defecto del modem, revisar qué dispositivos se conectan a tu red.

Referencias:

- https://myshadow.org/es/trace-my-shadow
- https://securityinabox.org/es/guide/firefox/windows
- https://securityinabox.org/es/guide/firefox/linux
- https://myshadow.org/es/tracking-data-traces
- https://cuidatuinfo.org/article/firefox-y-complementos-de-seguridad

Cómo hacer más segura tu computadora

Objetivo(s): identificar buenas prácticas para mantener nuestras computadoras seguras.

Módulo: Principios básicos de seguridad digital | Parte 1

Duración: 50 minutos.

Formato: Sesión.

Nivel de habilidades: Básico.

Conocimientos requeridos:
- Ninguno requerido.

Ejercicios/sesiones relacionadas:
- ¿Cómo funciona Internet? (Principios básicos de seguridad digital | Parte 1)
- Navegación segura (Principios básicos de seguridad digital | Parte 1)
- Malware y Virus (Principios básicos de seguridad digital | Parte 1)
- Almacenamiento y cifrado (Principios básicos de seguridad digital | Parte 2)

Materiales requeridos:
- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Copias impresas de la plantilla "Respaldo" (ver a continuación)

Recomendaciones:
- Recomendamos enfáticamente que documentes en vivo - utilizando un proyector conectado a la computadora - cualquier herramienta que vayas a cubrir en la sesión. Así, las participantes pueden seguir los pasos y replicarlos en sus computadoras con archivos "simulados" creados expresamente para la sesión (no archivos y datos importantes reales).

Conducir la sesión:

Parte 1 - Introducción

1. Pregunta a las participantes: qué valor tienen para ellas sus computadoras - ¿Qué tan útiles o esenciales son en su vida profesional y personal? ¿Cuánta información almacenan en ellas?

2. Ahora, pregunta: ¿Cuánto tiempo invierten en mantener su equipo? La diferencia entre el grado de valor que otorgan a sus dispositivos contra la cantidad de tiempo que dedican a cuidarlos y darles mantenimiento suele ser bastante amplia. Explica al grupo que la sesión se va a enfocar en prácticas básicas para proteger sus dispositivos.

Parte 2- Entornos físicos y mantenimiento

3. Comenta al grupo que muchas prácticas relacionadas con seguridad tienen, de hecho, más que ver con seguridad física que seguridad digital (esta aclaración es una buena manera de reforzar el enfoque holístico de esta currícula). Un buen ejemplo de ello es la importancia de limpiar los dispositivos (sacar polvo y otros residuos que quedan adentro) y realizar inspecciones físicas regulares del equipo para identificar si hay alteraciones o ha habido intentos físicos de acceso sin consentimiento. En este sentido, puedes recomendar prácticas digitales básicas como usar una contraseña para bloquear un dispositivo remotamente y también protección física como utilizar un protector de teclado o una cadena anti-robo para prevenir acceso sin consentimiento o hurto. Subraya el aspecto más crítico de la seguridad física de los dispositivos: tomar conciencia. Estar atenta a dónde está un dispositivo en cada momento - ya sea que lo traigas encima, en otro cuarto o en otro lugar seguro - es fundamental.

4. Pídeles a las participantes recordar los detalles de su espacio de trabajo. ¿Qué riesgos físicos pueden presentarse? ¿Está su computadora expuesta a ser robada? ¿Hay cables mal colocados? ¿Su computadora está bajo condiciones de calor o frío extremo o humedad? Estas consideraciones son importantes a la hora de estar conscientes - estar atenta a aspectos físicos de nuestros dispositivos no sólo es prevenir el acceso sin consentimiento sino también los daños potenciales que puede sufrir por el entorno.

Parte 3 – La seguridad de nuestro software

5. Explica a las participantes los riesgos de usar software pirata (alta probabilidad de descargar malware, más problemas para realizar actualizaciones que el software oficial, etc.); sin embargo, pagar software propietario generalmente sale caro. Puedes compartir varias referencias para abordar esta cuestión:

> **Osalt:** http://www.osalt.com
> Abre un navegador y entra en Osalt, un sitio web que presenta alternativas gratuitas y open source a la mayoría de las plataformas y suites de software propietarios (por ej. Ubuntu vs. Windows; LibreOffice vs. Microsoft Office; Inkscape vs. Adobe Illustrator)
>
> **TechSoup:** http://www.techsoupglobal.org/network
> A través de TechSoup, activistas de derechos humanos y organizaciones sociales pueden solicitar (a proveedores de servicios locales de TIC que son distribuidoras oficiales) versiones gratuitas o con descuento (para el sector público/sin ánimo de lucro) de software comercial. TechSoup coordina una red grande de distribución de donaciones de software - el enlace de arriba contiene una lista de socios y los países donde operan.

6. Explica la importancia de mantener el software actualizado - ante todo, les protege contra brechas de seguridad. Todo el software y actualizaciones deberán realizarse desde fuentes de confianza; por ejemplo, cuando actualices Adobe Acrobat Reader, sólo hazlo directamente desde Adobe y no sitios web de terceros.

7. Siguiente, explica la importancia de tener un programa de antivirus en la computadora. Brinda un poco de contexto para romper mitos comunes en torno a los antivirus como:

- *Utilizar dos o más me protege más.*
- *Mac y Linux no necesita antivirus porque no se infectan.*
- *Es totalmente seguro utilizar una versión pirata de software antivirus.*
- *Los programas antivirus gratuitos no son seguros o confiables como los de pago.*

8. Pueden comentar otros ejemplos que propongan las participantes. Después, discute algunas prácticas básicas de seguridad a la hora de utilizar software antivirus y protección contra malware (véase la sesión Malware & Virus de este módulo). Algunas prácticas útiles a subrayar aquí, en caso de no haberlas repasado en la sesión de Malware & Virus son:

- Utilizar el complemento uBlock Origin para evitar hacer clic en anuncios emergentes que pueden conducir a descargar archivos maliciosos en la computadora.
- Tomar conciencia sobre intentos de phishing, enlaces y adjuntos sospechosos contenidos en correos enviados a través de cuentas desconocidas o parecidas (pero no iguales) a las de nuestros contactos.
- Ahora es una buena oportunidad para comentar sobre cortafuegos (firewalls): ofrecen una capa de protección automática en nuestras computadoras. Comenta herramientas como "Comodo Firewall", "ZoneAlarm" y "Glasswire". Versiones más nuevas (con licencia) de Windows y Mac OS ya vienen con cortafuegos robustos pre-instalados.

Parte 4 – Protección de datos y respaldos

9. Pregunta a las participantes - ¿Con qué frecuencia realizan respaldos? Comparte experiencias de buenas prácticas relacionadas con el respaldo de datos, tomando en cuenta el tipo de información, como guardarlo en un lugar seguro, separado de la computadora, realizarlo con frecuencia, cifrar los datos y/o el disco entero.

10. Comparte la siguiente **plantilla** y pide a las participantes rellenarla. Explica que es un método útil para crear una política personal de respaldo de datos y volver a ella después del taller como un recurso de apoyo para seguir la pista a dónde almacenan sus datos y con qué frecuencia respaldar.

Plantilla para realizar respaldos

Tipo de información	**Importancia /Valor**	**¿Con qué frecuencia se genera/actualiza?**	**¿Cada cuánto se debería respaldar?**

11. Comenta, a continuación, que aunque existan herramientas para realizar respaldos automáticamente (como Duplicati.com o Cobian), puede ser más fácil para ellas empezar haciéndolo de manera manual arrastrando los archivos a respaldar al disco extraíble. Dependerá, en última instancia, de la complejidad y la cantidad de información que tengan que gestionar. Para la usuaria promedio, será suficiente con respaldar a mano.

12. A modo de seguimiento, repasa el concepto de cifrado para discos extraíbles. Explica qué implica y por qué es útil cifrar discos duros y discos extraíbles. VeraCrypt y MacKeeper, dos herramientas relativamente conocidas para cifrar archivos y discos, pueden ser opciones a explorar entre las participantes. En Linux pueden utilizar Duplicity para realizar respaldos cifrados automáticos.

Parte 5 - Borrado y recuperación de archivos
13. Lee en voz alta la siguiente afirmación:

Desde un punto de vista meramente técnico, no se puede borrar algo en tu computadora.

Pregúntale al grupo qué opina: ¿les hace sentido este enunciado? ¿Cómo puede ser que no exista una función de "borrado" real? Señala que puedes arrastrar un archivo a la papelera y después vaciarla, pero lo que hace eso realmente es borrar el icono y el nombre del archivo de un inventario escondido de todo lo que hay en tu computadora; y decirle a tu sistema operativo que puede ocupar ese espacio con otra cosa.

14. Pregúntales: ¿Qué crees que pasa con esos datos cuando se 'elimina'? Hasta que el sistema operativo vuelve a ocupar este nuevo espacio liberado, seguirá siendo utilizado por los contenidos eliminados, un poco como un archivador al que se le quitan las etiquetas, pero que mantiene los archivos originales.

15. Ahora explica que, debido a cómo una computadora administra el almacenamiento de datos, si tiene el software adecuado y ejecuta lo suficientemente rápido, puede restaurar la información eliminada de la misma manera. Existen herramientas parar eliminar de manera permanente (no sólo retirarlos del índice de archivos hasta que se ocupe el espacio). Aprovecha para presentar las herramientas **CCleaner, Eraser y Bleachbit** que sirven para eliminar de manera permanente archivos y el software **Recuva** para recuperarlos.

Referencias:

- https://securityinabox.org/es/guide/malware
- https://level-up.cc/curriculum/malware-protection/using-antivirus-tools
- https://securityinabox.org/es/guide/avast/windows
- https://securityinabox.org/es/guide/ccleaner/windows
- https://securityinabox.org/es/guide/backup
- https://securityinabox.org/es/guide/destroy-sensitive-information
- https://chayn.gitbooks.io/Avanzado-diy-Privacidad-for-every-woman/content/Avanzado-pclaptop-security.html

Privacidad

Nuestros dispositivos, nuestros datos - definir, comprender y reclamar el derecho a la privacidad en línea.

¡Pregúntame cualquier cosa!

Esta sesión está basada en el módulo desarrollado por Elis Monroy del colectivo Subversiones para el proyecto Voces de Mujeres.

Objetivo(s): Explicar cómo nuestros conceptos de privacidad cambian radicalmente en los espacios online.

Módulo Privacidad

Duración: 15 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Ejercicios y sesiones relacionadas:
- Privacidad (Privacidad)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a? (Privacidad)

Materiales requeridos:
- Diapositivas o tarjetas con preguntas (véase a continuación)

Recomendaciones:
- Es importante que compartas las indicaciones poco a poco conforme avance el ejercicio. Sigue el orden descrito a continuación. Si das todas las orientaciones al principio antes de arrancar con el ejercicio, ¡revelarás la sorpresa!
- Pregunta si se sienten en confianza hablando con el resto del grupo.

Conducir la sesión:

1. Las participantes escogen una pareja y buscan un lugar tranquilo para conversar.

2. Las preguntas detonantes son:
   - ¿Qué es la cosa más divertida o vergonzosa que te ha pasado?

- Comenta algo que detestas.
- ¿Tienes algún placer musical secreto?
- ¿Tenías un apodo de pequeña?
- ¿Quién es la persona más importante de tu vida?

Desde tu rol de facilitadora, puedes agregar o cambiar estas preguntas como veas necesario. El objetivo es romper el hielo: que emerjan anécdotas e información, quizás un poco vergonzosas o divertidas, para luego dar pie a hablar sobre la privacidad con el grupo. Puedes plantear más preguntas personales, siempre y cuando tengas en cuenta el contexto. Trata de no incomodar a las participantes.

3. Ahora se junta una pareja con otra. En total serán 4.

4. Cada participante presenta las respuestas de su pareja al otro par.

5. El grupo de 4 se junta con otro grupo de 4. Vuelven a repetir el proceso.

6. Pregúntale a las participantes cómo se sintieron en el ejercicio. Algunos temas que pueden haber salido son:

- Quizás algunas compartieron algo porque ya conocían a su compañera y se sentían cómodas aunque no anticipaban cómo iba a cambiar la dinámica.

- Una pareja presentó de una manera distorsionada a su compañera.

7. Termina la actividad hablando sobre la privacidad y cómo algunas personas aceptan los Términos de Servicio de una plataforma sin tener claridad de cómo son "las reglas del juego" y cómo van a cambiar a lo largo del tiempo. Aborda el tema de "consentimiento" y cómo una persona puede, a veces, aceptar que le tomen una foto, pero no expresó su acuerdo (consentimiento) a que esa foto se pudiera compartir online o con otras personas.

Referencias:

- https://labs.rs/en
- https://www.digitale-gesellschaft.ch/dr.html
- https://es-es.facebook.com/privacy/explanation

Privacidad

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.

Objetivo(s): introducir el concepto de privacidad e identificar información sobre nosotras mismas que está en Internet.

Módulo Privacidad

Duración: 50 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- Nuestros derechos, nuestra tecnología (Repensar nuestra relación con las tecnologías)
- ¡Pregúntame cualquier cosa! (Privacidad)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a?(Privacidad)
- Multitudes interconectadas (Privacidad)
- Hagamos doxxing al troll (Violencia en línea contra las mujeres)

Materiales requeridos:

- 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.

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 este 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 mismas.

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

Multitudes interconectadas

Esta sesión se basa en la investigación de Danah Boyd.

Objetivo(s): introducir el concepto de "multitudes interconectadas" para comprender mejor los aspectos clave e implicaciones de del papel, cada vez más protagonista, que juega la tecnología en la sociedad.

Módulo Privacidad

Duración: 20 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- ¡Pregúntame cualquier cosa! (Privacidad)
- Privacidad (Privacidad)
- Hagamos doxxing al troll (Violencia en línea contra las mujeres)
- ¿Qué dice tus metados sobre ti? (Activismo online más seguro)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados

Conducir la sesión:

1. Aclara que la sesión se centra en comprender mejor qué sucede cuando la tecnología se vuelve un componente cada vez más central y esencial de la sociedad y el impacto que tiene sobre la identidad y privacidad.

2. Para ilustrar esto, presenta conceptos clave que emergen en la investigación de Danah Boyd *"Taken Out of Context American Teen Sociality in Networked Publics"* (La sociabilidad adolescente fuera de contexto en multitudes interconectadas).

Multitudes interconectadas:
Son, simultáneamente, el espacio construído a través de tecnologías en red y el imaginario de comunidad que emerge como resultado de la intersección entre personas, tecnología y praxis.

Contenido de multitudes interconectadas:
Inherentemente constituido por bits, que son la unidad básica de la información digital. Tanto las auto-expresiones y las interacciones entre personas producen contenido de bits en multitudes interconectadas.

Cuatro características de las multitudes interconectadas:
Las características de los bits configuran las cuatro características claves de las multitudes interconectadas:

- ***Persistencia:*** *las expresiones online son registradas y archivadas automáticamente.*
- ***Replicabilidad:*** *los contenidos generados por los bits pueden ser duplicados.*
- ***Escalabilidad:*** *la visibilidad potencial de los contenidos es extendida.*
- ***Buscabilidad:*** *los contenidos pueden ser accedidos a través de búsquedas.*

Estas cuatro características estructuran las multitudes interconectadas y las interacciones que transcurren en ellas.

Dinámicas de multitudes interconectadas:
- ***Audiencias invisibles:*** *no todos los públicos son visibles cuando una persona contribuye online, ni están presentes a la vez necesariamente.*
- ***Contextos anidados:*** *la falta de fronteras espaciales, sociales y temporales hace difícil mantener contextos sociales separados.*
- ***Lo público y privado desdibujado:*** *sin control sobre el contexto, lo público y privado se torna un binario sin sentido, toma dimensiones nuevas y difícilmente pueden separarse.*

3. Explica y brinda ejemplos de cada una de estas características. Será útil que muestres ejemplos visuales.

Referencias:

- https://es.wikipedia.org/wiki/Bits

Apps & Plataformas online: ¿Amigo/a o enemigo/a?

Objetivo(s): identificar los tipos de información que compartimos con las apps y plataformas online que más utilizamos, diseñar estrategias y tácticas para utilizarlas de manera segura en nuestras ámbito personal y activismo online.

Módulo Privacidad

Duración: 120 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Principios básicos de seguridad digital y/o capacitación previa
- Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)
- ¿Cómo funciona Internet? (Principios básicos de seguridad digital | Parte 1)

Ejercicios y sesiones relacionadas:

- ¡Pregúntame cualquier cosa! (Privacidad)
- Privacidad (Privacidad)
- Multitudes interconectadas (Privacidad)
- Campañas online más seguras (Activismo online más seguro)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Papel (varias hojas por participante)
- Post-its (de varios colores)

Recomendaciones:

- Recomendamos que cada participante tenga acceso a internet desde su celular o algún otro dispositivo.

- Comparte materiales complementarios donde puedan aprender más sobre la privacidad en general y pasos que puedan tomar para afianzar su propia privacidad (véase sección de "Referencias" para enlaces).

Conducir la sesión:

Parte 1 – Nuestros dispositivos, nuestros datos

1. Las participantes revisarán todas las apps que tengan en sus dispositivos y verificarán lo siguiente:
   - ¿Quiénes son las personas que desarrollaron cada app?
   - ¿Cuáles tienen habilitada la función de geolocalización?
   - ¿Cuáles de las empresas propietarias de las apps podrían colaborar con las entidades gubernamentales locales?

2. Las participantes tienen 15 minutos para contestar. El grupo pone en común sus respuestas. Asegúrate de cubrir temas como los siguientes:
   - Permisos de apps que no parecen tener una relación clara con las funciones que se supone que tienen.
   - Términos de Servicios que son poco claras o ambiguas.
   - Políticas de Privacidad que permiten a las empresas vender los datos de las usuarias a otras empresas o instancias no declaradas claramente.

3. Comparte ejemplos de apps de menstruación ("menstruapps") - apps que ayudan a monitorear el ciclo menstrual - y otras apps relacionas con la salud personal. Explica que, según investigaciones como las de Chupadatos (https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/), se muestra que las menstruapps pueden recolectar bastante información personal sobre sus usuarias:

   - Nombre, número de teléfono y dirección.
   - Detalles sobre nuestro cuerpo como dolores menstruales, peso, horas de sueño.
   - Estados emocionales como estrés, falta de concentración o ansiedad.
   - Detalles sobre nuestra salud sexual, incluyendo métodos anticonceptivos.
   - Comportamientos online como los clicks que damos y los tipos de dispositivos que utilizamos.
   - Comportamientos offline como los medicamentos que tomamos o nuestros hábitos (tomar alcohol, fumar, etc.).

Es mucha información, ¿verdad?

Parte 2 - ¿Quién más nos está rastreando?

4. Divide las participantes en grupos de 3-4 (máximo) y pide a cada grupo que hagan una lista sobre qué saben de Facebook y Google. Pueden usar las siguientes preguntas como ayuda:

- ¿Cuál es la misión y los objetivos de estas empresas?
- ¿Qué servicios ofrecen?
- ¿Son servicios gratuitos o de pago?
- ¿Cuáles son las condiciones y términos de estos servicios?

Tienen 15 minutos para enumerar toda la información que se les ocurre.

5. Ahora anotan en otra lista qué creen que puede saber Facebook y Google sobre ellas. Si tienen acceso a Internet, las que tienen cuenta de Google pueden entrar en https://accounts.google.com/signin/v2/identifier?service=friendview&passive=1209600&hl=es&gl&continue=https%3A%2F%2Fwww.google.com%2Fmaps%2Ftimeline&flowName=GlifWebSignIn&flowEntry=ServiceLogin
para obtener más pistas. Tienen 20-25 minutos para hacer las listas. Después las presentarán al resto del grupo.

Parte 3 – Promover los derechos de las mujeres a través de plataformas de redes sociales

6. Las participantes permanecerán en los grupos de la actividad anterior. Cada grupo recibirá una serie de preguntas a discutir y trabajar juntas:

- ¿Qué herramientas y plataformas online utilizamos para organizar e intercambiar información de nuestros movimientos sociales, protestas y campañas? ¿Cuáles son algunas de las ventajas y desventajas de utilizar estas herramientas para estos propósitos?

- ¿Conoces ejemplos de censura de campañas y páginas en Facebook, videos en Youtube o cuentas de plataformas de redes sociales?

- Empresas como Facebook y Google son aliadas de los gobiernos y notorias por compartir información sobre sus usuarias. ¿Qué implicaciones tiene este hecho? (https://govtrequests.facebook.com sin referencia en español).

- ¿Conoces casos de violencia en línea contra mujeres? Específicamente, casos de amenazas en línea contra defensoras, difusión sin su consentimiento de desnudos o la creación de cuentas falsas en plataformas de redes sociales para desacreditarlas o "anunciar" servicios sexuales en su nombre, por ejemplo ¿En qué plataformas sucedió ésto y cómo reaccionó la empresa?

Los grupos tienen 10-15 minutos para contestar las preguntas. A continuación, se pone en común las respuestas de cada grupo.

7. Dedica 5-10 minutos en reflexionar sobre cómo estas mismas plataformas de redes sociales constituyen espacios de encuentro en internet. En este sentido, son escenarios ideales para implementar esfuerzos de campañas sociales. En última instancia, Facebook y los distintos servicios ofrecidos por Google brinda diferentes maneras útiles de interactuar con las seguidoras e integrantes de nuestras comunidad en línea; por lo tanto, a pesar de los aspectos preocupantes y desventajas que puedan emerger, es importante recordar que muchas de las participantes querrán seguir utilizándolas para acercarse a sus audiencias.

Parte 4 – Reclamar nuestra privacidad

8. Facilita el cierre de esta sesión. Veremos diferentes maneras de reclamar el derecho a la privacidad en línea y adoptar una manera más segura de utilizar las apps, plataformas de redes sociales digitales, tanto a nivel personal como en nuestros activismos.

9. Permaneciendo en los mismos grupos, ahora las participantes se centrarán en crear juntas una tormenta de ideas de maneras de reclamar su privacidad. Entrega a cada grupo una serie de post-its, marcadores y lapiceros/plumas. Tienen 10-15 minutos para anotar todo lo que se les ocurra. Puedes dar ejemplos de tácticas para arrancar como:

- Confundir a los algoritmos que las plataformas utilizan para mostrarte publicidad u optimizar contenidos.

- Verificar con frecuencia las políticas de privacidad y las actualizaciones de las configuraciones de privacidad de las plataformas.

- Prestar atención a los permisos otorgados a nuestros dispositivos, específicamente las configuraciones de geolocalización y ubicación de nuestras fotos y posts.

- Utilizar plataformas alternativas que están más comprometidas a respetar nuestra privacidad y activismo (Riseup, Tutanota, Signal, etc.).

Los grupos tendrán la oportunidad de compartir sus ideas. Puedes anotarlas en un lugar visible de la sala para que las participantes puedan volver a ellas a lo largo del taller. Estas ideas también serán útiles conforme vayas ajustando el contenido de tu capacitación, especialmente si las participantes quieren centrarse en usar de manera más segura las plataformas de redes sociales para su activismo.

Referencias:

- https://www.kaspersky.es/blog/digital-detox-advices/6226
- https://rankingdigitalrights.org/2017/08/30/rdr-en-espanol-guest-post
- https://myshadow.org/es
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
- https://www.digitale-gesellschaft.ch/dr.html
- http://www.europe-v-facebook.org/ES/Objetivos/objetivos.html

Activismo online más seguro

Pasar la voz y cuidar nuestra seguridad como mujeres y defensoras de derechos humanos online.

Sitios web más seguros

Objetivo(s): identificar prácticas más seguras para implementar y administrar nuestros sitios web, tanto sitios personales como sitios de activismo online y de nuestras organizaciones/colectivas/movimientos. Recuerda que hay muchas personas y organizaciones interesadas en atacar sitios web, no sólo los/as actores que identificamos como adversario/as. Existen personas que buscan sistemáticamente comprometer sitios web. Independientemente si identificamos a un/a agresor/a potencial, es importante mantener un nivel alto de protección en nuestro sitio.

Módulo Activismo online más seguro

Duración: 50 minutos

Formato: Sesión

Nivel de habilidades: Avanzado

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.
- Familiaridad con cómo se administran sitios web.
- ¿En quién confías? (Ejercicios para fortalecer la confianza)

Ejercicios y sesiones relacionadas:

- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a?(Privacidad)
- Campañas online más seguras (Activismo online más seguro).

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación).
- Computadora y proyector configurados.

Recomendaciones:

- Esta sesión será más relevante para algunos grupos que otros. Prioriza esta sesión especialmente para activistas y colectivos que tienen un sitio web.

- Prepara, desde antes, ejemplos (noticias y reportajes, posts de blogs, posts en plataformas de redes sociales, experiencias personales) de ataques en línea contra sitios web de defensoras y organizaciones de defensoras.

- Recuerda que, en algunos casos, las organizaciones no administran sus sitios o tienen limitaciones para realizar cambios, dependiendo de su estructura (ONG's internacionales, por ej.) De todas maneras, aún si no pueden incidir directamente en la gestión de su web, esta sesión les brindará una base sólida para que puedan empezar a pensar sobre los cambios que puedan necesitar (o incluso tomar control sobre su propio sitio).

Conducir la sesión:

Parte 1 – ¿Qué aspecto tiene un ataque online?

1. Arranca la sesión revisando algunas respuestas compartidas en la sesión de "¿En quién confías?" (Ejercicios para fortalecer la confianza) – en particular, comenta algunos de los posibles adversarios identificados por las participantes. Ésto brindará un contexto útil para abordar el tema de seguridad de sitios web, especialmente para activistas en espacios online.

2. Detona las siguientes preguntas:
   - ¿Qué consideran un ataque en línea?
   - ¿Qué casos de ataques online conocen?

   Si consideras oportuno, pregúntales si algún grupo o participante ha sido atacada en el pasado. También puedes compartir estudios de caso, previamente preparados para la sesión, si no surgen otros ejemplos.

3. Plantea las siguientes preguntas relacionados con los casos compartidos:
   - ¿El ataque surgió en el contexto de un evento específico como una protesta, la presentación de un informe u otro tipo de encuentro?
   - ¿Cuáles fueron las respuestas por parte de las defensoras involucradas?
   - ¿Se documentó el caso?

Parte 2 – Protegiendo y asegurando sitios web

3. Basándonos en los ejemplos, comparte algunas recomendaciones iniciales para mejorar la protección de sus sitios. Incluimos algunos ejemplos a continuación. Según los diferentes niveles de conocimiento en el grupo, quizás quieras ofrecer explicaciones más en detalle:

Opcional: *aunque haya participantes que estén familiarizadas con el manejo de sitios web, antes de proceder a recomendaciones, es buena idea explicar de qué maneras se puede administrar un sitio web. Algunos temas a cubrir aquí pueden ser: dominios, DNS, web hosting y sistemas de manejo de contenidos (CMS).*

Proteger tu sitio web

- Utiliza una contraseña de administradora robusta para evitar que comprometan tu sitio. El acceso indebido a sitios web, aprovechando contraseñas débiles, es uno de los ataques más comunes en este ámbito. Cuando sea posible, activa la autenticación de dos factores a la administración de tu sitio, cuenta de hosting y otros portales de acceso vinculados a tu sitio web.

- Cuando registras un dominio, generalmente te piden proporcionar datos como nombre, dirección postal y correo electrónico. Comprueba qué información queda disponible para los demás en tu registro de dominio (puedes hacer ésto buscando el dominio en 'whois.net') y considera optar por un registro privado de dominio.

- ¿Dónde está alojado geográficamente el dominio? Toma en cuenta lo siguiente:

    - ¿En qué país (incluso en qué ciudades) están localizados los servidores que alojan el dominio? ¿Puedes confiar tus datos al gobierno de dicho país y, más importante aún, puedes confiar en el servicio de hosting y de dominio en que no vaya a entregar tus datos ante una solicitud gubernamental? ¿Dicho gobierno podría intentar interferir con o intentar inhabilitar tu sitio?

    - Piensa dos veces si comprar tu dominio a una empresa que revende dominios. Ante una situación de ataque, vas a querer tener comunicación con el equipo de soporte para que te puedan ayudar. Algunas empresas son notorias por dar mal soporte técnico.

- Verifica qué plugins utiliza el sitio web. Un plugin es un programa que depende de otro y le agrega nuevas funciones. Wordpress, entre otros CMS, suelen integrar plugins. Asegúrate de sólo utilizar plug-ins cuando sea necesario y verifica que las que están habilitadas procedan de una fuente de confianza.

- Analiza si es apropiado, en tu caso, utilizar Jetpack (de Automatic) en tu Wordpress, especialmente para servicios como los widgets de plataformas de redes sociales y formularios de contacto. Existen plugins para hacer respaldos básicos de tu sitio como Better WP Security. Otros realizan respaldos automáticos como Vault Press o Backup Buddy.

- Procura actualizar con frecuencia tu CMS, plugins y las demás plataformas que estás administrando. Si tu servicio de hosting no realiza mantenimiento, asegúrate de cubrir ese aspecto directamente o a través de terceros de confianza.

Proteger las personas que navegan tu sitio

- Es altamente recomendable que tu sitio web ofrezca una conexión HTTPS por defecto (y no opcionalmente). Lets Encrypt de Electronic Frontier Foundation es un servicio que expide y verifica certificados de manera gratuita.

- Existen muchos colectivos en todas las latitudes que, desde las trincheras de las tecnologías, apoyan y se especializan en trabajar con organizaciones activistas. En Latinoamérica existen, por ejemplo, los proyectos Código Sur y Kefir.red. Otros colectivos afines son Autistici, NoBlogs y Blackblogs.org.

- Si alguna plataforma u sitio de una organización/colectivo/proyecto social sufre un ataque de denegación de servicio (DDOS), considera usar servicios como Deflect o Project Shield. Deflect es un proyecto de la organización sin ánimo de lucro, basada en Montreal, Equalit.ie. Ofrecen un servicio gratuito de mitigación de DDOS, avalado por la comunidad de seguridad digital.

- Investiga los plug-ins antes de instalarlos. ¿Qué reputación tienen las personas desarrolladoras? ¿Ha sido auditada (revisión de código)?¿Ofrecen soporte técnico? No instales algo sólo porque esté de moda.

Opcional: considera compartir información sobre cómo responder ante un ataque de DDoS. Ej: https://github.com/OpenInternet/MyWebsiteIsDown/blob/dev/MyWebsiteIsDown.md (Sin referencia en español)

Referencias:

- https://onlinesafety.feministfrequency.com/es/
- https://www.apc.org/es
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es

Campañas online más seguras

Esta sesión se basa en la guía desarrollada por Indira Cornelio para SocialTIC.

Objetivo(s): compartir recomendaciones de seguridad digital para defensoras de derechos humanos que están involucradas en esfuerzos de campañas online.

Módulo Activismo online más seguro

Duración: 50 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- ¿En quién confías? (Ejercicios para fortalecer la confianza)

Ejercicios y sesiones relacionadas:

- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- Modelo de riesgos con perspectiva de género (Buscando la mejor solución)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a?(Privacidad)
- Sitios web más seguros (Activismo online más seguro)
- Construyendo contraseñas más robustas (Principios básicos de seguridad digital | Parte 1)
- Malware & Virus (Principios básicos de seguridad digital | Parte 1)
- Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados

Recomendaciones:

- La intención de esta sesión es que las participantes identifiquen soluciones de seguridad digital con el fin de implementar prácticas más seguras a la hora de hacer campañas online; sin embargo, el objetivo final no es que las lleven a cabo durante la sesión, sino que empiecen el proceso de exploración de qué es más apropiado para sus contextos individuales.

Conducir la sesión:

Parte 1 – Introducción y planeación en prevención

1. Aclara a las participantes que la intención de esta sesión es que identifiquen soluciones de seguridad digital con el fin de implementar prácticas más seguras a la hora de hacer campañas online. No tendrán que implementarlas inmediatamente sino empezar a explorar cuáles son las más apropiadas para sus contextos y campañas.

2. Pídeles que compartan ejemplos de campañas online que conozcan. En su opinión, ¿existen tendencias emergentes?

3. Subraya que, a la hora de armar su campaña y hacer activismo en internet, deberían tomar en cuenta la información y lo/as adversario/as que identificaron durante la sesión de "¿En quién confías?". Las campañas, por ser esfuerzos llevadas a cabo en la esfera pública, implican prestar especial atención a quiénes podrían estarlas potencialmente monitoreando y amenazando en general.

4. Sugiéreles que, cuando se trata de arrancar con la fase de planeación de campaña en sus contextos de trabajo y acción, pueden trabajar en grupos las siguientes preguntas:

- ¿De qué trata la campaña?
- ¿A qué público se dirigen? ¿Cómo se sienten/cuál es su postura con respecto al tema que están tratando? ¿Están a favor o en contra?
- ¿Quiénes podrían sentirse expuestas o blanco de un ataque en esta campaña?
- ¿Cuáles podrían ser los argumentos potenciales que podrían formular contra la campaña?
- ¿Cuáles serían los mejores y peores resultados de esta campaña?

5. Responder estas preguntas puede ayudar a planear de manera más estratégica medidas preventivas ante posibles amenazas. Enfatiza que pueden hasta preparar mensajes respuesta por anticipado, tomando en cuenta posibles escenarios que pueden emerger. Los posibles escenarios positivos también pueden implicar planear medidas preventivas: por ejemplo, ¿cómo podrían prepararse ante la posibilidad que, si la campaña es un éxito y se vuelve muy conocida, su sitio web no pueda manejar tantas visitas y colapse?

6. Aclara que durante los siguientes pasos de la sesión, estarás brindando orientaciones y recomendaciones sobre prácticas de seguridad digital útiles para campañas online (si tienen tiempo, visiten sitios web de algunas herramientas).

Parte 2 – Proteger dispositivos

7. Pregúntales a las participantes si usan sus dispositivos personales para hacer sus campañas (vs. un dispositivo destinado específicamente a su "trabajo"). En caso afirmativo, ¿cuánta información relacionada con la campaña almacenan ahí? ¿Están conectadas, en el mismo dispositivo, a sus cuentas de correo y plataformas de redes sociales?

8. Algunas prácticas recomendables a destacar en este sentido son:

- **Poner contraseña** a sus computadoras y celulares.
- **Instalar un programa de antivirus** en sus computadoras y celulares.
- **Respaldar regularmente datos importantes y confidenciales** (registros de video, audio, anotaciones de entrevistas, informes, etc.) y guardar estos respaldos en lugares seguros que no estén cerca de sus dispositivos.

- **Habilitar el cifrado completo** de sus dispositivos
    - En caso de dispositivos móviles Android y Mac iOS, pueden habilitar esta función en la configuración del celular.
    - Para computadoras: Filevault para Mac OSX (https://es.wikipedia.org/wiki/FileVault) y BitLocker para Windows (https://es.wikipedia.org/wiki/BitLocker) son opciones comunes.
    - Aclaración: Filevault está ya instalado en Mac OSX sin coste adicional; sin embargo, BitLocker sólo viene de manera gratuita en Windows versión Pro, Enterprise y Education.

Parte 3 – Administrando accesos a tus cuentas

9. Las campañas online suelen requerir que varias personas accedan a una misma cuenta (o dispositivo, en algunos casos). Y ésto aumenta los posibles riesgos. Sin embargo, tomando algunas medidas preventivas, puedes reducir significativamente la probabilidad de que estos riesgos se traduzcan en amenazas:

- Para todas estas cuentas y dispositivos compartidos, limitar al máximo la cantidad de personas que tengan acceso es una de las primeras medidas críticas a implementar; otra medida es asegurarse que se sigan, de manera regular y consistente, los protocolos y procedimientos acordados (especialmente tomando en cuenta las recomendaciones a continuación).

- Particularmente en el caso de plataformas online, todas las personas que tengan acceso deberían verificar regularmente el historial y actividad de dichas cuentas. Por ejemplo, en cuentas de Gmail/Google, pueden verificar el historial de inicios de sesión recientes (y establecer alertas para actividades con patrones sospechosos) bajo la opción de "Última actividad de la cuenta"; de la misma manera, en Facebook, pueden ir al "Historial de actividad" bajo la opción de "Actividad reciente".

- Aplica prácticas básicas de contraseñas robustas para todos los dispositivos y cuentas que se van a utilizar en la campaña. Los administradores seguros de contraseñas como Keepass/KeepassX (http://keepass.info/) permiten crear bases de datos de contraseñas de cuentas. Esta base de datos se accede a través de una contraseña maestra. También recomendamos habilitar la autenticación de dos factores en Google, Facebook y Twitter para sumar una capa adicional de control de acceso.

- Si tienen que compartir una contraseña entre diferentes personas del grupo y no lo pueden hacer en persona, hazlo a través de opciones seguras como correo cifrado - con GPG o un servicio como Tutanota (https://tutanota.com/)- o chat cifrado (con la app Signal para celulares). Si utilizas Signal, asegúrate de establecer un protocolo de borrar historiales de chat o mensajes donde aparezcan estas contraseñas lo antes posible después de recibir la información requerida.

Parte 4 – Escoger apps para campañas

10. A la hora de implementar y organizar una campaña online, se acostumbra a utilizar determinadas apps y herramientas para monitorear las estadísticas de plataformas de redes sociales y sitios web; también para programar publicaciones. A la hora de escoger estas apps y tomar decisiones sobre ellas, tomen en cuenta las siguientes preguntas para evitar compartir información confidencial a través de herramientas inseguras o que ya no son mantenidas por el equipo desarrollador:

- ¿Esta app está siendo actualizada regularmente (funcionalidades, aspectos de seguridad, etc)?
- ¿El equipo desarrollador o el proyecto tiene cuentas en plataformas sociales para darle seguimiento e interactuar?
- ¿Qué dicen los demás sobre esta app?
- ¿Tienen blog? ¿Hay publicaciones recientes?

Parte 5 – Desarrollo comunitario a través de Facebook

11. Facebook es comúnmente utilizado en campañas online para organizar comunidades y difundir de manera rápida. Sin embargo, es importante subrayar algunas vulnerabilidades potenciales que emergen al utilizar estas plataformas como herramienta central de la campaña:

- Recomendamos que las participantes vayan tomando conciencia sobre las implicaciones que tiene usar Facebook (u otras plataformas de redes sociales hegemónicas) en su manejo de identidades en línea. Con el fin de limitar qué tanto se exponen, pueden crear perfiles específicos para administrar las páginas de su campaña y organización/colectivo/proyecto en vez de usar sus perfiles personales.
- Toma en cuenta que ahora puedes recibir notificaciones cifradas (con tu llave pública de GPG asociada a tu cuenta de correo) de Facebook. Esto puede ser útil para defensoras que quieren tomar más medidas a la hora de separar sus identidades.

- Es altamente recomendable que reflexionen sobre qué tipos de información y comunicaciones comparten. Existen ejemplos de páginas y perfiles de campañas en Facebook que han sido infiltradas por adversario/as, obligando a las administradoras a cerrarlas; y también casos donde Facebook ha cerrado estas páginas y perfiles por denuncias de terceros.

- Enfrentarse a una situación de censura puede ser un contratiempo significativo por lo que es importante **contar con canales alternativos de organización y comunicación como:**

    - Generar simultáneamente comunidades activas en otras plataformas para que siempre haya un alternativa/respaldo ante una contingencia;
    - Descarga la información de las páginas y los perfiles de la campaña en Facebook;
    - Usa listas de correos de Riseup (https://riseup.net/es/lists) para enviar boletines y otra información;
    - Organiza reuniones cara a cara cuando sea posible aunque, según el contexto, puede ser una opción arriesgada y poco aconsejable.

Parte 6 – Consentimiento informado

12. Discute la importancia del **consentimiento informado**, especialmente relevante en casos de campañas de concientización en derechos humanos donde se utilizan testimonios de víctimas, sobrevivientes y personas testigo de violencia y violaciones.

- Antes de registrar imágenes o videos de estas personas o documentar sus historias, debes pedir de antemano consentimiento explícito, para el registro en sí y para la **difusión pública** posterior. Informa a las personas para qué van a utilizar estos contenidos y cuáles son las posibles implicaciones de ello.

Referencias:

- http://seguridadigital.org/post/156287966318/consejos-de-seguridad-digital-para-gestionar-redes
- https://archive.informationactivism.org/es/index.html

¿Qué dicen tus metadatos sobre ti?

Objetivo(s): introducir el concepto de metadatos y la importancia de tomar conciencia sobre qué metadatos contiene cada tipo de contenidos, especialmente cuando estamos trabajando en situaciones de riesgo en el ámbito de derechos humanos.

Módulo Activismo online más seguro

Duración: 1 hora y 30 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- Multitudes interconectadas (Privacidad)
- Campañas online más seguras (Activismo online más seguro)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Ejemplos de herramientas para analizar y eliminar metadatos

Recomendaciones:

- Aunque no es necesario, esta sesión se puede aprovechar más si las participantes ya han repasado la sesión "Multitudes interconectadas".

- El tema de los metadatos es uno de los más complejos de presentar en los talleres de capacitación. Dedica suficiente tiempo a cubrir esta sesión en detalle ya que es bastante crítico y relevante en el contexto de defensoras y mujeres activistas.

Conducir la sesión:

Parte 1 - ¿Qué son los metadatos?

1. Arranca la sesión compartiendo algunos puntos clave:

- Comparte una definición de metadatos y dónde pueden encontrarlos comúnmente: imágenes, archivos Word y Excel, etc.

- Comparte algunos ejemplos típicos de metadatos (fecha, hora, ubicación donde el archivo fue creado, nombre de usuario/a o autor/a, tipo de dispositivo). Pueden verificar los metadatos de un archivo de su computadora o compartir capturas de pantallas de los metadatos que aparecen en los formatos de archivos más conocidos.

- Explica varias maneras en que se crean los metadatos y cómo pueden ser modificados/eliminados.

El tema de los metadatos es uno de los más complejos de presentar en los talleres de capacitación, así que asegúrate de preguntar si quedó clara la explicación y, si no fuera así, resolver dudas en profundidad.

Parte 2 - Implicaciones de metadatos en el contexto de derechos humanos

2. A la hora de trabajar con defensoras, es importante explicar las ventajas y desventajas de los metadatos. Puedes hacerlo a través de dos ideas clave:

Los metadatos pueden revelar mucho sobre ti.

- Tomen una foto con sus celulares y verifiquen todos los metadatos que contiene la imagen. Muéstrales la app CameraV y la herramienta web Metapicz (http://metapicz.com).

- Ahora vuelvan a tomar una foto, pero esta vez con la función de ubicación desactivada en sus celulares. Divide las participantes en grupos de 3 o 4 (máximo) para que discutan en qué sentidos creen que los metadatos pueden ser útiles y cómo pueden comprometer la seguridad de las personas que trabajan en derechos humanos.

- En la discusión grupal, mantén el enfoque en el trabajo de derechos humanos. Es importante que puedan identificar en qué circunstancias los metadatos contenidos en documentos, videos e imágenes puedan servir como evidencia a la hora de documentar casos de derechos humanos. Comparte algunas prácticas como guardar archivos originales en dispositivos cifrados y crear copias separadas para edición y almacenamiento en otras computadoras.

Los metadatos se crean, pero también pueden ser eliminados.

- Comparte varias opciones para borrar metadatos en videos e imágenes como ObscuraCam y Metanull. Si tienen suficiente tiempo, pueden probar eliminar los metadatos de documentos a través de LibreOffice.

Referencias:

- https://ssd.eff.org/es/module/por-qu%C3%A9-los-metadatos-son-importantes
- https://guardianproject.info/apps/obscuracam/ (Sin referencia en español)
- https://es.witness.org/recursos
- https://securityinabox.org/en/lgbti-mena/remove-metadata/ (Sin referencia en español)

Celulares más seguros

El conocimiento es poder. Cuanto más comprendemos sobre nuestros dispositivos móviles, más control tenemos sobre ellos.

Marco Polo

Este ejercicio está basado en la actividad "Marco Polo" creada por Fundación Karisma

Objetivo(s): ideal para explicar cómo funciona un celular y cómo recibimos mensajes SMS, llamadas y datos móviles en nuestros dispositivos.

Módulo Celulares más seguros

Duración: 15 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

3. Ninguno requerido

Ejercicios y sesiones relacionadas:

4. Multitudes interconectadas (Privacidad)
5. Campañas online más seguras (Activismo online más seguro)

Materiales requeridos:

- ¡Creatividad!

Conducir la sesión:

1. Escoge a alguien para interpretar el papel de "celular". Esta persona saldrá de la sala.

2. Aprovechando todo el espacio disponible, divide el resto del grupo en "edificios" y "antenas" e indica que se distribuyan por la sala. Asegúrate que las "antenas" se repartan uniformemente. Cada “antena” va a definir su propio "cuadrante".

3. El "celular" vuelve a entrar en la sala con los ojos cerrados. Tiene que localizar todas las "antenas" llamando en voz alta "Marco". Las antenas responden "Polo", pero sólo si pasa por su cuadrante. Los "edificios" permanecen silenciosas.

4. El "celular" intentará localizar todas las antenas. Después procede a explicar las funciones básicas de una red de telefonía celular:

- Los operadores de telefonía celular manejan antenas en diferentes áreas. Cada antena cubre una zona/cuadrante específico.
- Los celulares consiguen cobertura en la medida que envían peticiones a las antenas que se van encontrando (lo que en la dinámica se representa como “llamar a Marco”) al moverse de un lugar a otro. Las antenas responden ("Polo") entregando cobertura.

Celulares | Parte 1

Esta sesión es una adaptación de la actividad "¿Cómo funcionan los dispositivos celulares?" desarrollada por Alix Dunn (The Engine Room) para LevelUp.

Objetivo(s): brindar un repaso introductorio de cómo funcionan los celulares y las redes de telefonía celular.

Módulo Celulares más seguros

Duración: 60 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Ejercicios y sesiones relacionadas:
- Marco Polo (Celulares más seguros)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a?(Privacidad)

Materiales requeridos:
- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Papel

Recomendaciones:
- Esta sesión funciona mejor si realizan justo antes el ejercicio "Marco Polo" del mismo módulo; sin embargo, pueden llevarla a cabo independientemente.

Conducir la sesión:

Arranca explicando los componentes claves de los celulares. Puedes mostrar imágenes como apoyo visual.

Parte 1 - ¿Qué compone un celular?

1. Aunque algunos celulares, especialmente los smartphones, tienen funcionalidades avanzadas, todos comparten algunos componentes comunes:

Antena

Permite comunicar con otros dispositivos móviles y redes externas. En los dispositivos más antiguos hasta puede ser visible (y retráctil). Los celulares más nuevos tienen antenas integradas y no se aprecian a primera vista. La antena es responsable de comunicarse con la red de telefonía y la red WiFi. Estas funciones las puede cumplir una sola antena o una para cada tipo de red.

Batería

Almacena energía que alimenta el dispositivo celular; en la mayoría de los celulares, se puede retirar. En algunos smartphones más nuevos (sobre todo en los iPhones y los modelos nuevos de Samsung Galaxy S) la batería no está diseñada para acceder a ella fácilmente. Es importante tener ésto en cuenta porque justamente nos interesa poder retirarla como método de seguridad.

Microprocesador banda base

Administra las comunicaciones, incluyendo los comandos que la usuaria realiza con el celular y el celular con la red de telefonía. Esta banda base suele ser patentada por los fabricadores: una "caja negra" inaccesible y difícilmente manipulable. La banda base determina la capacidad de poder, desde una red de telefonía, encender tu celular, identificar su ubicación, activar el micrófono y descargar datos del dispositivo.

Tarjeta y ranura SIM

Lugar donde se almacena la tarjeta SIM en el celular. Tu tarjeta SIM tiene una capacidad limitada de almacenamiento. Puedes decidir guardar determinados datos en tu tarjeta SIM , en la memoria interna o en una unidad de memoria extraíble. Algunos celulares están diseñados para administrar múltiples tarjetas SIM; los teléfonos que no operan en redes GSM (generalmente CDMA) no tienen tarjeta SIM.

IMEI

Identificador numérico, generalmente único, de celulares 3GPP, iDEN y algunos celulares satelitales. Puedes ubicar este número en la etiqueta de la batería, marcando en el teclado *#06# o en las configuraciones de sistema del sistema operativo smartphone. Tenga en cuenta que, aunque cambies la tarjeta SIM, no cambia tu IMEI y tu proveedor de telecomunicaciones puede acceder a él.

Medios extraíbles
Cualquier tipo de memoria externa que pueda ser introducida y extraída de un dispositivo móvil; generalmente son tarjetas SD y micro-SD. Algunos celulares también cuentan con puertos infrarrojo (IR) y/o Bluetooth que mandan datos a través de rayos de un teléfono a otro.

Cámaras
Con la mayoría de los celulares puedes tomar fotos y/o video, en particular con los smartphones. Muchos tienen cámaras frontales y traseras para poder realizar llamadas de video.

Parte 2 – Sesión práctica

2. Las participantes trabajarán en parejas y crearán una lista de amenazas que pueden surgir a través del uso de dispositivos móviles. Después anotarán recomendaciones de prácticas que creen que pueden ayudar a asegurar dichos dispositivos, tomando en cuenta los distintos componentes descritos anteriormente en la parte 1.

3. Las participantes se juntan de vuelta y ponen en común. Algunas de las prácticas y herramientas que pueden surgir son (si no las cuentan los grupos, preséntalas)

- Antivirus
- VPNs
- Comprobar la configuración de apps
- Contraseñas robustas
- Respaldo de datos
- No cargar celulares vía USB en computadoras públicas

4. Comenta la complejidad de mejorar la seguridad de los celulares. Esta cita de Levelup es un buen ejemplo de ello:

Este componente administra las comunicaciones, incluyendo los comandos que la usuaria realiza con el celular y el celular con la red de telefonía. La banda base de los celulares suele ser patentada por los fabricadores: una "caja negra" inaccesible y difícilmente manipulable.

Aunque esta cita hace referencia al sistema operativo ”banda base”, se trata de una problemática común a otros componentes de los celulares.

A modo de ejercicio, es útil discutir la legislación en materia de comunicaciones de los contextos regionales de las participantes.

El tema de las apps es fundamental. La falta de preocupación que tienen las usuarias en relación con quiénes desarrollan las apps que utilizan es un riesgo latente. Podrían abordar esta discusión haciendo paralelismos con cómo escogemos libros, comida, marcas, etc.

Referencias:

- https://securityinabox.org/es/guide/mobile-phones

Celulares | Parte 2

Objetivo(s): introducir herramientas y recomendaciones para mejorar la seguridad que tienen las participantes, ya familiarizadas con conceptos básicos de seguridad digital, con sus celulares.

Módulo Celulares más seguros

Duración: 50 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

6. Marco Polo (Celulares más seguros)
7. Celulares | Parte 1 (Celulares más seguros)
8. Introducción al cifrado (Cifrado)
9. Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

Ejercicios y sesiones relacionadas:

10. Marco Polo (Celulares más seguros)
11. Celulares | Parte 1 (Celulares más seguros)
12. Apps & Plataformas online: ¿Amigo/a o enemigo/a? (Privacidad)
13. Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

Materiales requeridos:

14. Diapositivas (con los puntos claves descritos a continuación)
15. Computadora y proyector configurados

Recomendaciones:

- Si es posible, averigua de antemano qué tipo de celulares utilizan las participantes. Puedes preguntarles en la fase de diagnóstico, por ejemplo. Ésto te ayudará a adaptar la sesión a los dispositivos y sistemas operativos que manejan.
- Antes de comenzar el taller, repasa algunas prácticas básicas de seguridad digital para celulares: software antivirus, VPNs, verificar las configuraciones y permisos de acceso de las apps.
- **Indícales a todas que hagan un respaldo de todos sus archivos antes de arrancar la sesión** para que puedan hacer pruebas en sus propios celulares sin arriesgar a perder su información.

Conducir la sesión:

Parte 1 – Cifrado para celulares

1. Repasa el concepto de cifrado que ya vieron en la sesión de "Introducción al cifrado" y quizás en la sesión de "Cómo hacer más segura tu computadora". Comenta que las versiones más actuales de iOS y Android (mayo 2017) tienen cifrado habilitado por defecto.

Parte 2 – Usar GPG en el celular

2. Si las participantes ya están familiarizadas con el cifrado GPG, introduce directamente el cliente de correo K-9 y la app APG. Discute las ventajas y desventajas de usar GPG en el celular (especialmente el riesgo de guardar tu llave privada GPG en tu smartphone y las vulnerabilidades específicas de los celulares). La idea principal de esta parte de la sesión es recalcar que las decisiones dependen del contexto: las participantes tendrán que sopesar qué es más apropiado para ellas en su situación.

Opcional: *deja tiempo para que puedan instalar y practicar con K9 y APG. Quizás quieran crear un nuevo par de llaves GPG y probarlas en estas apps.*

Parte 3 - ¿Tu celular te está rastreando?

3. Pregúntales a las participantes: ¿cuánta información tienen nuestros celulares sobre nosotras? Los celulares son un medio para mantener conversaciones con otras personas; por lo tanto, nuestros celulares tienen acceso a toda o casi toda nuestra comunicación. De la misma manera, los celulares también monitorean nuestros contactos. Cada conversación que realizamos en nuestro celular se vincula a individuos específicos.

4. Este tipo de monitoreo es un tipo de vigilancia que sucede en nuestro cotidiano. Quizás quieran discutir sobre ello. Qué tipo de amenazas y riesgos pueden emerger a la hora de utilizar sus celulares, especialmente en su contexto específico como defensoras.

Referencias:

- https://securityinabox.org/es/guide/mobile-phones
- http://www.zeit.de/datenschutz/malte-spitz-data-retention (sin referencia en español)

Anonimato

Analizar de cerca la línea difusa entre los espacios físicos y virtuales nos ayuda a recuperar control sobre nuestras identidades.

Amistad secreta

Objetivo(s): explicar el concepto de anonimato y dirigir una sesión práctica que genere mayor conciencia sobre su relevancia.

Módulo Anonimato

Duración: 30 minutos (dependiendo del tamaño del grupo)

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- Anonimato (Anonimato)
- ¡Más identidades en línea! (Anonimato)

Materiales requeridos:

- Lapiceros, materiales de papelería y sobres
- Sillas
- Un cuenco o una jarra
- Tiras pequeñas de papel
- Una venda o algo para tapar los ojos

Recomendaciones:

- Recomendamos explicar de antemano lo que implica el siguiente ejercicio. Puesto que el tiempo es limitado, el ejercicio se aprovechará mejor si las participantes imaginan de antemano las identidades que van a crear.

Conducir la sesión:

Parte 1 - Introducción

1. Cada participante compartirá una identidad totalmente nueva para si misma (la cual habrán preparado antes de la sesión). Tiene que ser totalmente inventada (y no basada en alguna persona).

2. Al construir esta nueva identidad, las participantes podrán ejercer una libertad total: pueden ser una mujer, un hombre, hasta un lugar... lo que se les ocurra. El punto clave aquí es desarrollar en detalle su nueva identidad: nombre, de dónde vienen, su trabajo, familia, aficiones, etc.

Parte 2 - ¡Vamos a jugar!

3. Repasa por encima el concepto de anonimato. Pregúntales a las participantes por qué creen que el anonimato puede ser importante en el trabajo que realizan y en su vida personal.

Facilita la siguiente parte a través de estos pasos:

4. Cada quien tiene que tener en mente todos los detalles de su personaje: nombre, de dónde vienen, su familia, sus aficiones, etc. Pide a cada una antes de empezar el taller que te diga el nombre de su personaje para que puedas tomarlo en cuenta a la hora de facilitar el juego.

5. Cada una escribe en una tira de papel el nombre de su personaje. Toma todas las tiras y colócalas en un recipiente.

6. Muévete por la sala e indica a cada participante retirar una tira de papel. Si les toca su propio personaje, deben devolver el papel y retirar otro. El nombre del papel que tiene cada una es su amiga secreta.

7. Tienen varios minutos para escribir una carta a su amiga secreta describiendo (desde su nuevo personaje) quiénes son, de dónde vienen, qué les gusta, etc.

8. Colocan esta carta en un sobre y escriben el nombre de su amiga secreta en la parte exterior del sobre. Asegúrate que las participantes no vean lo que las demás escriben para evitar revelar detalles,

9. Toma todos los sobres y entrégalos a las personas correspondientes. Las participantes leen su carta sin ver los nombres de los demás sobres.

10. Una por una, cada participante se levanta y se sienta en una silla delante del grupo con los ojos vendados. Comparte con el grupo el contenido de la carta que recibieron, incluyendo el nombre de su amiga secreta.

11. Conforme va describiendo, la amiga secreta se levanta y se sienta en una silla al lado.

12. Una vez que termine la descripción, la participante intenta adivinar quién cree que es su amiga secreta. Retira la venda y se fija en la persona que tiene a su lado para verificar si acertó.

13. Repite estos pasos para cada uno de los personajes.

Parte 3 - Cerrar el círculo

Pregunta al grupo si acertaron quién era su amiga secreta. ¿Cómo consiguieron adivinarla? ¿Cuál fue la ruta de pensamiento que siguieron? ¿Qué tan difícil fue para ellas?

14. Cierra el ejercicio animando una reflexión sobre la importancia del anonimato y ser capaz de proteger íntegramente nuestra identidad, también cómo puede ser fácil, a veces, ocultar nuestras identidades e intenciones reales.

Anonimato

Objetivo(s): introducir el concepto de anonimato en línea, además de herramientas y prácticas relevantes que puedan ayudar a preservar dicho anonimato.

Módulo Anonimato

Duration: 40 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.

Ejercicios y sesiones relacionadas:

- Amistad secreta (Anonimato)
- ¿Qué dicen tus metados sobre ti? (Activismo online más seguro)
- Navegación más segura (Principios básicos de seguridad digital | Parte 1)
- ¡Más identidades en línea! (Anonimato)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados

Conducir la sesión:

Parte 1 – Introducción al anonimato online

Arranca la sesión con la siguiente pregunta: ¿Qué significa el anonimato para ti? Después de varias contribuciones del grupo, presenta más en profundidad el concepto.

Explica cuáles son los beneficios de aprender más sobre el anonimato y por qué es relevante para nuestro trabajo en derechos humanos.

Brinda ejemplos de rastros digitales en línea que pueden identificarnos. Estos rastros pueden incluir datos como nuestro nombre de usuaria, posts de plataformas de redes sociales, dispositivos utilizados, ubicaciones y otros tipos de metadatos.

Platica cómo el anonimato puede ser aplicado en distintos niveles: a una actividad, una conexión, un perfil o sesión entera.

Parte 2 – Identificar datos y preservar el anonimato

2. En la primera parte de esta sesión, discutimos distintos tipos de rastros de datos en línea que pueden identificarnos. Ahora subrayaremos un rastro en concreto, especialmente relevante en el contexto de nuestra actividad online: nuestra dirección IP.

¿Qué es una dirección IP? Explica qué es, su finalidad y cómo puede ser un dato fundamental (especialmente cuando intentemos navegar de manera anónima).

Pueden usar un sitio web como https://whatismyipaddress.com/ para descubrir su dirección IP y otros tipos de datos confidenciales que nos pueden identificar.

3. Presenta las siguientes herramientas y cómo son importantes a la hora de preservar nuestro anonimato en línea. Cada herramienta funciona de una manera distinta:

- Navegador Tor
- Red Privada Virtual (VPN: Virtual Private Network)
- Tails (Sistema Vivo Amnésico e Incógnito/The Amnesiac Incognito Live System)

Es importante que destaques las prácticas clave a considerar en el uso de cada herramienta y dar suficiente tiempo para instalar y practicar cada una de ellas.

Parte 3 – Sesión práctica

4. Las participantes volverán a verificar su dirección IP en https://whatismyipaddress.com/: una vez desde una VPN y después desde el Navegador Tor. ¿Notaron cambios en la dirección IP o en otra cosa?

5. Aprovechando, presenta también el "modo incógnito". Muchas veces, las usuarias piensan que están navegando de manera anónima cuando usan el modo incógnito en sus navegadores. Invita a las participantes a verificar su dirección IP en dicho modo (o el equivalente a modo incógnito en los otros navegadores). ¿Qué notaron de diferente en su dirección IP ahora?

Referencias: https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

¡Más identidades en línea!

Esta sesión está basada en la guía de "Creando y gestionando identidades en línea" del manual "Zen y el arte de que la tecnología trabaje para ti" del colectivo Tactical Tech.

Objetivo(s): revisar ejemplos de casos, herramientas y buenas prácticas para crear identidades en línea.

Módulo Anonimato

Duración: 120 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.
- Anonimato (Anonimato)
- ¿Qué dicen tus metados sobre ti? (Activismo online más seguro)
- Navegación más segura (Principios básicos de seguridad digital | Parte 1)

Ejercicios y sesiones relacionadas:

- Anonimato (Anonimato)
- Amistad secreta (Anonimato)
- ¿Qué dice tus metados sobre ti? (Activismo online más seguro)
- Navegación más segura (Principios básicos de seguridad digital | Parte 1)

Materiales requeridos:

- Computadora y proyector configurados
- Rotafolio (1 ó 2 hojas por participante)
- Marcadores, lapiceros/plumas

Conducir la sesión:

Part 1 – Connected Online Identities

1. Cada participante crea una lista de todas las identidades en línea que tiene; también puedes simplificar esta parte preguntándoles si alguna tiene más de una identidad online. A las que responden que "sí", pregúntales si se sentirían cómodas compartiendo por qué lo hacen y para qué usan sus distintas identidades.

2. Basándote en los ejemplos y experiencias que salieron, explica que utilizar varias identidades online es una práctica común entre defensoras. Brinda varios escenarios cuando ésto sucede:

- Defensoras que usan Facebook para administrar campañas en línea, pero no quieren usar su perfil o identidad personal.

- Defensoras que realizan investigación confidencial y quieren dejar el menor rastro digital posible que las pueda identificar.

- Defensoras que han estado documentando casos de abuso de derechos humanos por parte de entidades gubernamentales y planean publicar información de manera pública (informe, comunicado, etc).

3. El grupo se divide en parejas e identifican juntas otras circunstancias en las que sería útil crear una nueva identidad que no estuviera vinculada a la suya personal. Reflexionan en qué medida mezclan sus identidades personales con su activismo.

- ¿Combinan sus cuentas? ¿Cómo?
- ¿Hasta qué punto vinculan su vida digital personal con su vida activista?
- ¿Cuáles son algunas de las actividades online que podrían ponerlas en riesgo y exponerlas si estuvieran usando sus identidades reales? Ejemplos podrían ser:
    1. Solicitudes de información a agencias gubernamentales.
    1. Visitar sitios de entidades gubernamentales y recopilar información que comparten online.
    1. Administrar cuentas de plataformas de redes sociales de su organización/colectiva.

Parte 2 – Separar y administrar identidades en línea

4. De nuevo, partiendo de las reflexiones que salieron en el grupo en el paso anterior, comparte 3 opciones a la hora de gestionar tus identidades en línea:

- Crear una identidad totalmente nueva y falsa en línea.
- Crear perfiles personales y profesionales separados.
- Dejar tu identidad tal cual como está ahora (no cambiar nada).

5. Para cada opción, brinda al menos un ejemplo real y relevante y explica sus implicaciones:

- Crear una identidad totalmente nueva y falsa en línea probablemente va a requerir, para que sea un método eficaz, desconectarte completamente de cualquier cosa relacionada con tu identidad real. Ésto implica crear una nueva cuenta de correo y cuenta de plataforma de red social, entrar y salir de tus sesiones de cuenta (de manera consistente, es decir, siempre) y, en caso de cuentas de plataformas de sociales, empezar de 0 sin ningún seguidor/a.

- Separar identidades profesionales de las personales puede sólo requerir cambiar la configuración de privacidad de tus cuentas, ya sea para limitar la cantidad de información que está disponible públicamente o para administrar específicamente qué nivel de información está visible para determinadas amistades, seguidores/as o contactos; en otros casos, sin embargo, separar estas identidades podría implicar mantener una serie de perfiles y cuentas totalmente separadas (lo que significa que tendrían que crear todo una serie de cuentas -correo, plataformas de redes sociales, etc- o para tu identidad profesional o para tu identidad personal).

- Dejar tu identidad tal cual como está ahora solo requiere que verifiques la configuración de privacidad de tus cuentas, ya sea para limitar la cantidad de información que está disponible públicamente o para administrar específicamente qué nivel de información está visible para determinadas amistades, seguidores/as o contactos.

6. Las parejas discutirán entre ellas algunas ventajas y desventajas de cada una de estas opciones, ya sea en un sentido general o en sus contextos específicos. Algunos temas que pueden salir es el criterio de practicidad y credibilidad. Debes estar preparada para abordar estas cuestiones en el grupo.

Parte 3 – Sesión práctica y recomendaciones

7. Las participantes podrán escoger cualquiera de las tres opciones presentadas antes en el ejercicio aunque el siguiente ejemplo descrito está basado en la opción de crear una identidad totalmente nueva.

8. Entrega a cada participante 1 ó 2 hojas de papel de rotafolios y algunos marcadores. Esbozarán las características de su nueva identidad. Algunas consideraciones que pueden tomar en cuenta son:

- ¿Qué nombre van a utilizar? (Presta atención que en algunas plataformas de redes sociales, como Facebook y Google, pueden identificar y bajar cuentas con nombres falsos, así que van a tener que ser creativas).
- ¿De dónde son y dónde viven?
- ¿Qué avatar o foto de perfil van a utilizar?

- ¿Algunos de los detalles podrían identificarlas?

9. Comparte algunas recomendaciones de seguridad digital que podrían ayudarlas a evitar exponer sus identidades reales. Toma en cuenta que algunas de estas recomendaciones ya fueron explicadas y abordadas en otras sesiones (requeridas para esta sesión) como las sesiones "Anonimato", "¿Qué dicen tus metadatos sobre ti" y "Navegación segura".

- Utiliza un celular desechable ("burner") para crear nuevas cuentas y perfiles sin asociarlas a tu número personal. Google te pide un número de teléfono para recibir códigos de verificación a la hora de sacar una cuenta. También lo necesitarás para configurar la autenticación de 2 factores para la mayoría de las plataformas (este sistema de inicio de sesión/autenticación es muy recomendable en algunos casos ,para aumentar la seguridad de tus cuentas). Si quieres preservar tu "anonimato", no uses la autenticación de dos factores porque implica que ese teléfono desechable esté reportando tu ubicación geográfica a la operadora de telefonía. También es importante tomar en cuenta que utilizar una nueva tarjeta SIM en el mismo teléfono no te otorga anonimato.

- Utilizar diferentes máquinas o dispositivos para cada identidad -al igual que se comenta arriba- ayuda a separar identidades y actividades sin que cometamos errores que podrían comprometernos al crear una nueva identidad. Usar computadoras y celulares separados, configurar una máquina virtual en nuestra laptop o utilizar otro sistema operativo como Tails (veremos ésto en la sesión "¡Empezar de vuelta!"). Cuando estemos creando un nuevo perfil, idealmente cuando vayamos a iniciar sesión en estas cuentas en el futuro, considera utilizar diferentes navegadores web en modo incógnito de tal manera que evites vincular tus cuentas o accidentalmente entrar en la sesión equivocada y compartir información que podría comprometer tu protocolo de seguridad. Aunque toma en cuenta que si te estás conectando desde una misma dirección IP, tu proveedor de internet puede asociar tu actividad en línea.

- Cuando estén creando un perfil nuevo, e idealmente cuando estén iniciando sesión a cuentas asociadas en el futuro, las participantes deberían toma en cuenta utilizar distintos tipos de navegadores. Ésto les ayudará a evitar vincular cuentas entre sí o accidentalmente loguearse a la cuenta equivocada.

- Repasa prácticas generales de navegación segura. Puedes tocar el tema de "huellas de navegador" y el impacto que tienen a la hora de separar cuentas (https://panopticlick.eff.org/static/browser-uniqueness.pdf); también puedes mostrar cómo esconder tu ubicación cambiando la dirección IP de tu dispositivo.

- Es desaconsejable que te suscribas a tus páginas y los perfiles de tus amistades, familia o a los grupos a los que perteneces (organizaciones, colectivos, etc.) desde tu nueva identidad porque podrían trazar conexiones entre tus identidades.

- Subraya la importancia de los metadatos y cómo pueden revelar información sobre nosotras mismas. Vuelve a explicar cómo se crean los metadatos y cómo pueden eliminarlos de sus archivos antes de publicar imágenes o videos, o antes de enviar archivos desde sus nuevas cuentas.

8. ¡Las participantes crean perfiles y cuentas para sus nuevas identidades en línea!

Referencias:

- http://www.dominemoslatecnologia.org/apc-aa-files/cf8592edd1e1521f99a367712f16a8f8/manual-de-instalacion-de-obscuracam.pdf

Cifrado

A la hora de proteger nuestros datos y comunicaciones de miradas fisgonas, nosotras, y sólo nosotras, somos guardianas de las llaves de nuestra información.

Introducción al cifrado

Objetivo(s): explicar el concepto de cifrado, repaso breve de diferentes tipos de cifrado.

Módulo Cifrado

Duration: 50 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.

Ejercicios y sesiones relacionadas:

- Privacidad (Privacidad)
- Campañas online más seguras (Activismo online más seguro)
- Comunicaciones cifradas (Cifrado)
- Almacenamiento y cifrado (Principios básicos de seguridad digital | Parte 2)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados

Recomendaciones:

- **Este infográfico puede ser útil:**
  https://emailselfdefense.fsf.org/es/infographic.html

Conducir la sesión:

Parte 1 - ¿Alguna vez has cifrado?

1. Aclara que esta sesión es una introducción al cifrado, así que no van a profundizar sobre herramientas de cifrado que las participantes pueden ya haber escuchado (como GnuPG).

2. Divida las participantes en parejas y arranca la sesión mostrando algunos ejemplos de técnicas de cifrado. Prepara estos ejemplos de antemano.

El código BLUEPRINTS
Cada una de las letras de la palabra "blueprint" tiene un número asignado.

R E F E R E N C I A
0 1 2 3 4 5 6 7 8 9

Aunque este ejemplo se basa en una palabra determinada, puede aplicarse a cualquier secuencia de letras y palabras. Por ejemplo, si usas el mismo sistema que el de arriba, la secuencia de números **82579** deletrea la palabra **TURNS** cuando se descifra.

También puedes cambiar el orden de los números, de tal manera que quedaría así:

R E F E R E N C I A
9 8 7 6 5 4 3 2 1 0

En este ejemplo, la secuencia de números **82579** ahora deletrea ECRFR (que no es una palabra) cuando se descifra; sin embargo, podrías "descifrar" la secuencia 903210 como **RANCIA.**

Mensajería de texto a la antigua
Utiliza una imagen de un teclado (véase abajo) para demostrar otro tipo de "cifrado" con las que se puedan familiarizar las participantes.

Pregúntales cómo utilizarían ese teclado para deletrear diferentes palabras, por ej, sus nombres. El nombre Luisa se deletrearía con la secuencia **5 5 5 8 8 4 4 4 7 7 7 7**

3. Pregunta si han usado otros tipos de cifrado, parecidos a los ejemplos de antes o cualquier otro tipo que se les ocurra (ej. usar conexión HTTPS).

4. Cierra la sesión planteando otra pregunta: ¿Cuáles son los elementos comunes con los que se pueden identificar a partir de estos diferentes ejemplos de cifrado?

5. Toma en cuenta que algunos servicios de correo electrónico como Gmail tienen que ser configurados para permitir el uso de Thunderbird como aplicación de terceros.

Parte 2 - Explicar el cifrado
6. Basándote en los elementos que salieron en la parte 1, amplía sobre los principios y prácticas básicas:

- **Métodos de cifrado:** dedica tiempo a explicar cómo funciona el cifrado, refiriéndote a ejemplos de la parte 1 y mostrando capturas de pantalla sobre el aspecto que tiene un correo cifrado con GnuPG. Destaca implementaciones conocidas de cifrado, en particular, repasa con tiempo el HTTPS, el cifrado punta a punta y el cifrado GPG/PGP.

- **Llaves y pares de llaves:** explica cómo funcionan los pares de llaves y la relación algorítmica entre llaves públicas y privadas. Vuelve a repasar los ejemplos de implementaciones comentados anteriormente (HTTPS, el cifrado de punta a punta y el cifrado GPG/PGP) y explica, en cada caso, dónde se almacenan las llaves y cómo visualizarlas.

- **Prácticas de cifrado:** destaca buenas prácticas clave asociadas a las implementaciones conocidas de cifrado como el verificado de huella y la firma de llaves. A modo de demostración, pide a las participantes localizar en Signal la opción de verificado de huella de usuaria; de la misma manera, si las participantes ya tienen llaves GPG/PGP, pueden discutir las ventajas y desventajas de firmar y distribuir llaves públicas. Aprovecha para discutir la mensajería cifrada punta a punta para apps de mensajería instantánea como Signal, Telegram y Whatsapp. Aclara que el cifrado de punta a punta en algunos servicios no está habilitado por defecto.

- **Respaldos cifrados:** partiendo del ejemplo de GPG/PGP de arriba, pregunta si piensan que es buena idea realizar un respaldo de su llave privada GPG y si es sí, ¿cómo lo harían?

Referencias:

- **https://www.gnupg.org/gph/es/manual/book1.html**

Comunicaciones cifradas

Objetivo(s): partiendo de los contenidos formativos anteriores sobre cifrado, en esta sesión se transmite la importancia y utilidad de cifrar comunicaciones y se brindan herramientas relevantes.

Módulo Cifrado

Duration: 50 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.
- Introducción al cifrado (Cifrado)

Ejercicios y sesiones relacionadas:

- Introducción al cifrado (Cifrado)
- Privacidad (Privacidad)
- Campañas online más seguras (Activismo online más seguro)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados

Conducir la sesión:

1. Comparte ejemplos relevantes de situaciones donde la comunicación cifrada es útil y dedica tiempo a explicar cómo funciona el cifrado. Muestra capturas de pantalla de correos cifrados con GPG para ilustrar por encima qué aspecto tienen los mensajes y correos cuando están cifrados. También destaca implementaciones conocidas de cifrado - en particular, HTTPS, cifrado de punta a punta y cifrado GPG/PGP.

2. Centra la discusión en herramientas que permiten cifrar comunicaciones. Ejemplos buenos son: Signal para llamadas y mensajes, meet.jit.si para llamadas de video, Tutanota o GPG+Thunderbird para correos.

3. Explica los beneficios a nivel de seguridad de estas herramientas, sobre todo, cómo permiten a las usuarias limitar el acceso que otras personas tienen sobre sus comunicaciones; después discute situaciones donde la seguridad de los datos de la usuaria podrían ser comprometidas, aún estando cifradas. Pregunta: ¿cómo podría comprometerse un correo cifrado con GPG a través de registradores de teclas o malware que captura la pantalla? ¿Y si un/a adversario/a consigue nuestra llave privada de GPG? ¿Cómo podrían acceder a nuestros datos?

4. Si tienen tiempo, pónganse manos a la obra con al menos dos de las herramientas comentadas en el paso 2. Aunque no tengan tiempo para repasar GPG/PGP para email, pueden optar por mostrar cómo hacer llamadas de video cifradas vía HTTPS a través de meet.jit.si o instalar Signal en los celulares para practicar enviar mensajes cifrados entre sí o realizar llamadas cifradas.

Referencias:

- https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-ios

Principios básicos de seguridad digital | Parte 2

Almacenar y asegurar la información que más atesoramos y saber cuando resetear.

Almacenamiento & Cifrado

Objetivo(s): reforzar la importancia de realizar respaldos regulares de nuestros datos y discutir cómo prevenir la manipulación y acceso sin consentimiento a nuestra información.

Módulo Principios básicos de seguridad digital | Parte 2

Duración: 90 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.

1. Introducción al cifrado (Cifrado)
2. Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

Ejercicios y sesiones relacionadas:

3. Privacidad (Privacidad)
4. Campañas online más seguras (Activismo online más seguro)
5. Introducción al cifrado (Cifrado)
6. Cómo hacer más segura tu computadora (Principios básicos de seguridad digital | Parte 1)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Copias impresas de la plantilla "Respaldo" (ver a continuación)
- USB's u otro tipo de unidades extraíbles (para cada participante)

Recomendaciones:

- En esta sesión, usaremos Veracrypt o Luks (según el sistema operativo) para practicar el cifrado de respaldos y unidades extraíbles. Para ahorrar tiempo, descarga los instaladores antes de la sesión.

- En general, y especialmente en el caso de las principiantes, no recomendamos cifrar todo el disco de la computadora aún. Mejor prueben Veracrypt o Luks con unidades extraíbles (como una USB) utilizando archivos de prueba, preparados especialmente para esta sesión. No quieres correr el riesgo de que una participante pierda acceso a todos sus datos durante el taller sin querer. Puedes preparar USB's de antemano con archivos de prueba y descargar instaladores de 32 y 64 bits de Veracrypt.

Conducir la sesión:

Parte 1 – Respaldo de datos y planeación

1. Pregunta a las participantes: ¿Con qué frecuencia realizan respaldos? Comparte ejemplos de buenas prácticas de respaldo de datos como guardar el respaldo en un lugar seguro alejado de la computadora, hacerlo con cierta frecuencia y -según el tipo de información que quieren respaldar- considerar cifrar su disco duro o disco extraíble donde se va a almacenar los datos.

2. Comparte la siguiente plantilla y pide a las participantes rellenarla: Explica que es un método útil para crear una política personal de **respaldo de datos** y volver a ella después del taller como referencia que nos ayude a seguir la pista a dónde almacenamos nuestros datos y con qué frecuencia respaldamos.

Plantilla para realizar respaldos

Tipo de información	**Importancia/ Valor**	**¿Con qué frecuencia se genera/actualiza?**	**¿Cada cuánto se debería respaldar?**

Parte 2 – Almacenamiento y cifrado de respaldos

3. Una vez que hayan rellenado las plantillas, invítalas a repasar de nuevo los diferentes tipos de información (y su respectiva relevancia/valor) en las listas que crearon, tomando en cuenta qué pasaría si esa información cayera en las manos de nuestros adversario/as o si se perdiera por completo. ¿Qué tipo de impacto tendría a nivel personal o a nivel de nuestra organización?

4. Introduce el concepto de cifrado y lo cotidiano que es en realidad: es utilizado en las diferentes herramientas y plataformas con las que interactuamos cada día. HTTPS, por ejemplo, es una forma de cifrado de datos "en tránsito" (los datos viajan de un punto A a un punto B). En esta sesión revisaremos el cifrado de datos "en reposo" (información que se almacena en un lugar).

5. Recuerda a las participantes que se les indicó desde antes descargar Veracrypt o MacKeeper en sus computadoras. Dé tiempo a que lo instalen y prueben con datos de prueba (creados expresamente para la sesión). Sobre todo para principiantes, no es recomendable que cifren todo el disco duro interno de su computadora aún. No queremos correr el riesgo de que una participante pierda acceso a todos sus datos durante el taller sin querer.

Referencias:

- https://securityinabox.org/es/guide/veracrypt/windows
- https://securityinabox.org/en/guide/veracrypt/mac
- https://securityinabox.org/es/guide/veracrypt/linux

¡Empecemos de nuevo!

Objetivo(s): reforzar la idea que "las herramientas y tecnologías no tienen poderes sobrenaturales sobre nosotras! Acompañarás a las participantes por un proceso de empoderamiento: aprenderán a resetear sus dispositivos "desde cero".

Módulo Principios básicos de seguridad digital | Parte 2

Duración: 90 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.
- Introducción al cifrado (Cifrado)
- Almacenamiento & Cifrado (Principios básicos de seguridad digital | Parte 2)

Ejercicios y sesiones relacionadas:

- Impresiones personales sobre la seguridad (Repensar nuestra relación con las tecnologías)
- Malware & Virus (Principios básicos de seguridad digital | Parte 1)
- Privacidad (Privacidad)
- ¡Más identidades en línea! (Anonimato)
- Almacenamiento & Cifrado (Principios básicos de seguridad digital | Parte 2)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- USBs vivos configurados con sistemas operativos Tails y Ubuntu

Recomendaciones:

- Considera entregar una USB a cada participante para que se quede con ella; si no hubiera USB's para todas, prepara varias computadoras, tanto con Tails como con Ubuntu para que puedan probarlas porque, aunque sea sólo para probar desde la USB, algunas participantes puedan sentirse incómodas probándola en su propia máquina.

- Esta ejercicio puede adaptarse y ser una sesión por si misma si hay interés por parte del grupo en migrar de sistema operativo completamente (de Windows o Mac OS a una distribución de Linux como Ubuntu).

Conducir la sesión:

Parte 1 – Disipando el mito

1. Arranca explicando el objetivo de esta sesión: reafirmar el poder que tienen las personas sobre las tecnologías, disipando la noción que los dispositivos digitales tienen "poderes mágicos" sobre sus usuarias. Si ya llevaste a cabo la sesión "Impresiones personales sobre la seguridad", puedes recordar varios puntos clave:

¡Las herramientas y la tecnología no tienen poderes mágicos sobre nosotras! Nosotras somos quienes decidimos cuándo accedemos a ellas, sin embargo, es muy difícil tener control al 100% de los dispositivos que utilizamos y debemos tener mucho cuidado.

Parte 2 – ¿Qué significa empezar de vuelta (resetear)?

2. Repite la afirmación anterior y enfatiza la última frase "siempre podemos empezar de vuelta, aprendiendo de las experiencias anteriores". ¿Qué significa eso? Explica ofreciendo el siguiente escenario:

- Quizás, en algún momento de tu experiencia con la seguridad digital, has sentido que lo estabas haciendo todo mal.
- Tu computadora está llena de programas, películas, series pirata y un montón de otros archivos que ni recuerdas haber descargado.
- Has conectado un sinfín de USB's sin ningún criterio en tu computadora y otras computadoras, incluyendo en espacios públicos como cibercafés. A veces hasta sacas la USB sin extraerla de manera segura.
- Quizás acabas de terminar una relación con alguien que sabes, a ciencia cierta, estaba mirando tu computadora cuando tú no estabas. Probablemente adivinaron tu contraseña o puede ser que se lo diste.
- Ahora te sientes fuera de control. ¿Quién sabe los tipos de virus están viviendo en tu disco duro o quién tiene acceso a tu información?

- Pero sabes qué: todo está bien. No es demasiado tarde para empezar de nuevo. ¿Vamos? Esta sesión es para ti.

3. Explica qué significa "resetear" en este contexto: significa empezar de cero haciendo un "reset" de tu dispositivo o computadora para volver a su estado y configuración inicial por defecto.

Es muy importante que consideres esto: “resetear” los dispositivos restaura la configuración original, pero no restaura información perdida ni recupera datos que fueron expuestos a personas no autorizadas.

Pedagógicamente, esto te brinda una "hoja en blanco" para tu proceso de seguridad digital.

Asegúrate de recordar a las participantes que en esta sesión explicarás cómo realizar un "reset". No van a tener que hacerlo ellas mismas durante la sesión ni en el resto del taller.

Hacer un reset puede salir mal si las participantes no están preparadas o no han hecho un respaldo de sus datos recientemente. Seguramente querrán también utilizar sus laptops tal como están ahora para mantener el acceso a sus datos mientras se preparan mejor.

Sin embargo, durante esta sesión, las participantes tendrán la oportunidad de practicar utilizando sistemas operativos alternativos en sus computadoras, punto importante para prepararse para el momento que decidan hacer un reseteo.

Parte 3 – Check-in:¿Necesito hacer un respaldo?

4. Idealmente, ya habrán realizado la sesión "Almacenamiento & Cifrado" ya que aborda puntos clave con respecto a respaldo de datos. De cualquier manera, antes de empezar la parte práctica de esta sesión, haz un breve repaso con el grupo sobre cómo respaldar sus datos.

Opcional: *pregúntales a las participantes con qué frecuencia respaldar sus archivos. Comparte ejemplos de buenas prácticas de respaldo de datos como guardar el respaldo en un lugar seguro alejado de la computadora, hacerlo con cierta frecuencia y -según el tipo de información que quieren respaldar- considerar cifrar su disco duro o disco extraíble donde se va a almacenar los datos.*

Parte 4 – Resetear& Reiniciar

5. Antes de comenzar con la parte práctica de la sesión, otro punto clave a abordar es la relación entre reiniciar y resetear, dos términos que pueden usarse como si fueran la misma cosa.

Se refieren a procesos muy parecidos en un sentido más general, pero recuerda que "resetear" se utiliza para ilustrar el concepto de "empezar de nuevo" en el contexto de esta sesión.

Reiniciar es una operación técnica que realizarán con sus computadoras durante el reseteo. Es importante que comprendan cómo funciona.

6. Profundizando en esta idea, presenta Tails y Ubuntu como sistemas operativos alternativos a Mac OS y Windows. En esta sesión, aprenderemos a utilizarlas a través de una usb.

Parte 5 – Sistema operativo vivo

7. Quizás te pregunten: ¿Cómo vamos a utilizar un nuevo sistema operativo en nuestras computadoras sin desinstalar la que tenemos ahora? ¿Qué pasará con nuestros datos? Aprovecha para explicar algunos términos que puedan ayudarlas a entender mejor cómo funciona Tails y Ubuntu.

Sistema vivo
Sistema operativo que corre directamente desde un disco extraíble como una USB o una tarjeta SD. Tails (Sistema Vivo Amnésico Incógnito // Amnesic Incognito Live System) es un ejemplo de sistema vivo; Ubuntu, otra variación de Linux, también puede ser configurado como sistema vivo.

Linux
Sistema operativo similar a Windows o Mac. La diferencia principal es que su código está abierto (opensource) y se distribuye de manera gratuita. Por ello, existen muchos tipos de adaptaciones de Linux disponibles. Debian, una de las distribuciones más conocidas es la base del desarrollo de Tails.

Dispositivo de arranque o “booteable”
Dispositivo o disco desde el cual una computadora carga archivos para poder arrancar. En la mayoría de los casos, el dispositivo booteable de una computadora es su disco duro interno. Desde aquí se carga el sistema operativo cuando prendes tu computadora. Aparte de los discos duros, los CDs, DVDs, tarjetas SD y USBs pueden ser también dispositivos de arranque.

BIOS
El Sistema Básico de Entrada-Salida (Basic Input/Output System) es el primer software que la mayoría de las computadoras corren cuando las prendes. Realizan pruebas en la máquina para asegurarse de que el sistema y el hardware esté funcionando correctamente y después inicia la secuencia de carga para el software (como el sistema operativo) disponible en el dispositivo booteable. El BIOS tiene una interfase, pero las usuarias no tienen acceso a ella al menos que sigan una serie de pasos determinados durante el arranque del sistema.

Secuencia de arranque

Puedes accederla a través del BIOS (o UEFI) durante el arranque de la computadora. Se trata de una lista de dispositivos booteables de la computadora y sirve para determinar el orden en que la computadora intentará cargar información. Generalmente, el disco duro interno es el primer dispositivo en la secuencia a cargar el sistema operativo. Sin embargo, se puede cambiar esta secuencia para cargar primero información de un disco externo/extraíble como un DVD o un USB.

Parte 6 – Sesión Práctica

8. Divide las participantes en al menos dos grupos. Dale a cada grupo una computadora para que intenten correr Ubuntu o Tails desde un usb vivo. Si tienes suficientes USBs preconfigurados para entregar a cada participante, pueden practicar estos pasos por su cuenta.

9. Repasa cada paso desde tu computadora, proyectando la pantalla en la pared. Muéstrales el proceso de reiniciar sus computadoras y arrancar desde el sistema vivo Tails o Ubuntu durante la secuencia de arranque BIOS. Conforme vayas mostrando, asegúrate de explicar las diferencias entre Tails y Ubuntu para que el grupo pueda entender mejor cómo pueden ser utilizados para "empezar de vuelta".

10. Cierra la sesión conversando sobre cómo el hecho de resetear usando Tails o Ubuntu puede ser una opción para "pasar de hoja" cuando hayamos vivido un ataque de malware o perdido control. También procura comentar otros tipos de ataque donde ésto no es una solución, como tal, por ejemplo, en caso del acoso en línea.

Referencias:

- https://tails.boum.org/ (Sin referencia en español)
- http://www.ubuntu-es.org

Violencia en línea contra las mujeres

Reconocer - y luchar en contra de - patrones de acoso y abuso que enfrentan las defensoras de derechos humanos en línea.

Espectograma

El contenido de este ejercicio fue desarrollado por Mariel Garcia (SocialTIC) y Spyros Monastiriotis (Tactical Technology Collective).

Objetivo(s): este ejercicio brinda una manera útil para que las participantes conozcan sus posturas y reflexiones sobre determinados temas a través de la creación de un "espectograma" de opiniones.

Módulo Violencia en línea contra las mujeres

Duración: 15 minutos (según el tamaño del grupo)

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- Una Internet Feminista (Violencia en línea contra las mujeres)

Material requerido:

- Una sala grande o un espacio exterior
- ¡Tú misma!

Conducir la sesión:

1. Arranca indicando dónde se ubican los dos extremos del Espectograma. Si están en un espacio interior, puede ser los dos extremos de la sala; si están afuera, puede ser la distancia entre dos árboles, paredes u otros puntos de referencia.

2. Cada uno de estos extremos representa una postura: "muy de acuerdo" y "muy en desacuerdo".

3. Explica el ejercicio: leerás en voz alta un enunciado (es importante plantearlas como afirmaciones y no como preguntas) y la volverás a repetir; las participantes se organizarán a lo largo del espectro "Muy de acuerdo-Muy en desacuerdo" según su postura con respecto a la afirmación. Evita confusiones y no uses frases que contengan doble negación.

4. Recuerda a las participantes que no tienen que escoger sólo un extremo u otro del espectro; pueden ubicarse en el punto medio si están indecisas o en cualquier punto según su nivel de acuerdo o desacuerdo con el enunciado.

5. En este espectrograma, la facilitadora leerá en voz alta varios enunciados relacionados con la seguridad digital y experiencias de mujeres en línea. Algunos ejemplos podrían ser:

No hay un motivo de peso para compartir la contraseña de tu cuenta de correo o de plataforma de red social.

A veces es necesario que nosotras, como mujeres, evitemos compartir ciertos puntos de vista online.

Tanto hombres como mujeres activistas enfrentan el mismo tipo de violencia y amenazas online.

Mi trabajo se hace imposible sin acceso seguro a espacios online.

6. Cada vez que las participantes se ubican en un punto del espectro al escuchar un enunciado, pide a 2 o 3 participantes que compartan su postura. Estas aportaciones pueden detonar una discusión muy interesante.

7. Las participantes podrán cambiar de lugar después de haber escuchado los puntos de vista de las compañeras. Si sí lo hacen, pregúntales por qué.

Una Internet Feminista

Objetivo(s): brindar una oportunidad para generar conciencia sobre los retos que afrontan las mujeres en internet.

Módulo Violencia en línea contra las mujeres

Duración: 40 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- Her-Story (las historias de las mujeres) de las tecnologías (Repensar nuestra relación con las tecnologías)
- Violencia simbólica (Violencia en línea contra las mujeres)

Materiales requeridos:

- Rotafolio o papelógrafos
- Marcadores de colores
- Copias de Principios Feministas de Internet (http://www.genderit.org/es/articles/principios-feministas-para-internet) para cada participante

Conducir la sesión:

Parte 1 – Generar conciencia

1. Arranca la sesión preguntándole a las participantes: ¿cuáles son algunos de los mensajes e ideas más comunes que han escuchado sobre mujeres y tecnologías? ¿Cuáles son las actitudes predominantes en relación a mujeres y tecnologías en sus países/contextos?

2. Las participantes crean una lluvia de ideas con algunos de los obstáculos que las mujeres afrontan cuando intentan acceder a las tecnologías y/o participan activamente en espacios en línea. Pueden hacerlo todas juntas o en grupos más pequeños. Como quieran. Anota las aportaciones del grupo(s) en el rotafolio.

3. Comparte algunas estadísticas generales y, si es posible, algunas más específicas en relación con las regiones y países de las chicas:

- La penetración de uso de internet es más alto en el caso de hombres que mujeres en todas las regiones del mundo. La brecha de género es del 12%.

- El 60% de los casos de violencia de género relacionado con las tecnologías digitales no es investigada por las autoridades.

- Entre el 84 y 91% de los editores de Wikipedia son hombres.

- Las mujeres ocupan el 27% de los puestos relacionados con gestión y dirección dentro de empresas de media y un 35% de la plantilla que trabaja en el sector de redacción.

- Las mujeres que trabajan en tecnologías digitales ganan 28% menos que sus compañeros hombres, teniendo la misma formación, años de experiencia y edad.

4. Divide las participantes en grupos pequeños y pídeles reflexionar sobre las estadísticas compartidas anteriormente. ¿Cuáles son las implicaciones que tienen en las vidas de las mujeres y en la construcción de un internet como espacio común que podamos habitar libremente?

Parte 2 - Principios feministas de internet

5. Introduce los "Principios feministas de internet de APC" como detonante de una reflexión sobre

> ***(…) una internet feminista que se encamine hacia el empoderamiento de más mujeres y personas queer que puedan ejercer y disfrutar sus derechos, interactuar con placer y de manera lúdica; y desmantelar el patriarcado.***

6. Entrega a cada grupo materiales impresos de los principios.

- Acceso
- Movimientos y participación pública
- Economía
- Expresión

- Agencia

7. Pide a cada grupo discutir cómo cada principio se aplica en sus contextos y que hagan una lista de las maneras en que cada una pueda contribuir a transformar las realidades de las mujeres y las tecnologías.

8. Cada grupo presentará lo que haya reflexionado en conjunto y las conclusiones sacadas.

Referencias:

- http://feministinternet.net
- https://es.wikipedia.org/wiki/Brecha_de_g%C3%A9nero_en_Wikipedia
- https://www.apc.org/es/pubs/principios-feministas-para-internet-version-2

Violencia simbólica

Objetivo(s): cómo identificar la violencia simbólica y cómo esbozar conexiones entre ella y la violencia de género en línea.

Módulo Violencia en línea contra las mujeres

Duración: 30-45 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- Espectograma (Violencia en línea contra las mujeres)
- Una Internet Feminista (Violencia en línea contra las mujeres)

Materiales requeridos:

- Rotafolio
- Marcadores, lapiceros
- Hojas de colores
- Post-its
- Cinta adhesiva

Conducir la sesión:

Parte 1 - ¿Qué es la violencia simbólica?

1. Arranca explicando qué significa el término "violencia simbólica".

La violencia simbólica se ejerce a través de imposiciones culturales de normas y comportamientos en relación al género. Se enseñan a las mujeres que "algo" nos puede pasar si andamos solas de noche, nos vestimos de cierta manera o si hacemos algo sin precaución. El miedo se convierte en un estado mental normalizado y aceptado.
Esto implica que a nosotras, en tanto mujeres, nos responsabilizan por cualquier violencia que enfrentamos. Se engendra un estado de miedo y hasta terror que dibuja un "mapa mental de espacios prohibidas" para nosotras y suscita respuestas condicionadas como:

- *Sentir la necesidad de volver a casa de noche en un taxi o con un compañero varón.*
- *Caminar más rápido o hasta corriendo cuando escuchamos pisadas detrás de nosotras.*
- *Auto-censurarnos sin darnos cuenta en plataformas de medios sociales u otros tipos de plataformas.*
- *Decidir no salir a la calle o no vestirnos de cierta manera por miedo a lo que nos podría pasar.*

Además, no sólo nos hacen responsables por la violencia que vivimos sino que no nos brindan estrategias y recursos para abordarla (aparte de las respuestas condicionadas de arriba), ni a disfrutar y ocupar los espacios, ni a ser libres en cómo nos movemos y hablamos en nuestros cuerpos y en nuestras sexualidades.

La violencia simbólica crea espacios y situaciones prohibidas para las mujeres y nos niega nuestro derecho fundamental a la seguridad y a la libertad de movimiento. La impunidad de los agresores es un agravante a toda esta situación. A menudo, dichos agresores no son cuestionados sino patologizados como "locos" o inheremente incapaces de tomar control o responsabilidad sobre sus acciones.

Llegando a este momento de la sesión, quizás quieras discutir algunos imaginarios de la violencia que se ejerce contra las mujeres (violencia simbólica u otros tipos), normalizada por los medios de comunicación, especialmente en espacios online.

Parte 2 - Identificar la violencia simbólica contra nosotras mismas.
2. Entrega a cada participante post-its e indícales que anoten ejemplos de actividades que han dejado de hacer y comportamientos que han cambiado fruto de la violencia simbólica que han experimentado como mujeres ocupando espacios offline y online. Reúne de vuelta los post-its y lee algunos de los ejemplos en voz alta. Discútelas todas juntas, reflexionando sobre las posibles motivaciones detrás de estos cambios.

3. Explica que hay tres principales factores que construyen y habilitan el miedo y el terror en respuesta a la violencia simbólica:

- **La apropiación del cuerpo femenino:** el cuerpo femenino es visto como un objeto en un entorno masculino; ésto genera una ausencia de seguridad y confianza de la mujer hacia su cuerpo y sus capacidades.

- **Culpa y vergüenza:** consideradas como elementos permanentes e inamovibles que facilitan la percepción de que violencia de género perpetrada es merecida y, de cierta manera, aceptable.

- **"Felicidad aprendida":** estado psicológico que se genera con frecuencia cuando los eventos son percibidos como incontrolables, como si no se pudiera hacer nada para cambiar las consecuencias. El estado mental se adapta a través de la aceptación y normalización: sacrificamos nuestra agencia de tomar el control de vuelta.

4. Pregunta a las participantes qué estrategias creen que podrían transformar estos factores y abordar la violencia simbólica. Las pueden anotar en sus post-its. Compartimos algunas posibles estrategias:

- Recuperar el control sobre la narrativa de nuestro cuerpo a través de resignificarla como territorio de placer y resistencia.

- Reconocer y aceptar los daños que han sido ejercidos contra nuestro cuerpo (física y mentalmente), no como víctima sino como sobreviviente resiliente.

- Construir y sostener redes de apoyo para nosotras, tanto online como offline. Nunca estamos solas en la lucha.

Referencias:

- https://es.wikipedia.org/wiki/Indefensi%C3%B3n_aprendida
- http://www.autodefensafeminista.com/attachments/article/277/MANUAL%20Autodefensa%20Feminista.pdf

Denunciando el abuso en plataformas de medios sociales

Objetivo(s): compartir consejos para denunciar la violencia en línea que se ejerce en plataformas de redes sociales como Facebook y Twitter.

Módulo Violencia en línea contra las mujeres

Duración: 40 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Ejercicios y sesiones relacionadas:

- Campañas online más seguras (Activismo online más seguro)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a? (Privacidad)
- ¡Empecemos a crear un diario de documentación! (Violencia en línea contra las mujeres)

Materiales requeridos:

- Proyector y diapositivas
- Post-its
- Una computadora por cada dos participantes (si es posible)

Recomendaciones:

- Esta sesión está especialmente dirigida a mujeres que han sido acosadas en línea o que están involucradas en campañas online.

Conducir la sesión:

1. Arranca la sesión preguntando a las participantes:

- ¿Conocen colectivos de mujeres o activistas mujeres que hayan sido acosadas en línea?
- Si es así, ¿en qué plataformas?

Pídeles que comparten ejemplos de tácticas que han visto que se utilizan o han utilizado ellas para afrontar el acoso en línea y que las escriban en post-its.
2. Comparte algunas recomendaciones de prácticas básicas para denunciar tipos de violencia comúnmente ejercidos contra las mujeres online, además de ONGs y colectivos que pueden brindar apoyo.

- La empresa Facebook recomienda reportar el comentario/post específico, dando el máximo contexto posible. Pueden leer sobre este proceso aquí: https://www.facebook.com/report

- Bloquear acosadore/as evita que recibamos solicitudes de amistad/suscripción o inicios de conversaciones, envío de mensajes o que dicha persona vea nuestras actualizaciones. Facebook no te notifica cuando te bloquean, pero te puedes dar cuenta en la medida que ya no puedes contactar con la otra persona.

- Toma capturas de pantalla antes de bloquear a quien/quienes te acosan para documentar pruebas del acoso porque, una vez que lo/as bloqueas, se hace más difícil recopilar evidencias que puedas tener que presentar en una futura investigación sobre el incidente. Enseña a las participantes a sacar capturas si no saben hacerlo.

- Twitter recomienda reportar el incidente y mantener el registro del número de caso para dar seguimiento. En Twitter puedes reportar tanto un tweet individual como un perfil entero.

- Es recomendable evitar entrar en los links que te envían tu(s) acosadore/a(s), ya que pueden dirigirte a la instalación de malware en tu dispositivo.

3. Muestra cómo bloquear usuario/as y reportar perfiles y posts en Facebook y Twitter, además de otras plataformas de redes sociales que utilicen las participantes. Asegúrate de investigar estos procedimientos antes del taller para estar actualizada de cómo se hace. Estos procedimientos tienden a cambiar bastante (al igual que las configuraciones de privacidad).

4. Si quieres dedicar un tiempo a que las participen prueben por si mismas, divídelas en grupos pequeños e índicales que busquen páginas o perfiles que pueden ser blanco de acoso en línea. Pueden, por ejemplo, documentar posts o perfiles en Facebook que están propinando, de manera sistemática, acoso y reportarlas.

Referencias:

- https://karisma.org.co/descargar/manualseguridadtw

¡Empecemos a crear un diario de documentación!

Objetivo(s): introducir prácticas que profundizan en la denuncia de abuso en línea, especialmente en el ámbito de la documentación de incidentes.

Módulo Violencia en línea contra las mujeres

Duración: 45 minutos

Formato: Sesión

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Ejercicios y sesiones relacionadas:
- Denunciar el abuso en plataformas de redes sociales (Violencia en línea contra las mujeres)
- Hagamos doxxing al troll (Violencia en línea contra las mujeres)

Materiales requeridos:
- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Copias impresas de la plantilla "Respaldo" (ver a continuación)

Recomendaciones:
- Orientada a grupos que afrontan acoso en línea, han recibido amenazas online y offline, o que van a trabajar en proyectos o campañas que aumentan el riesgo a estar expuestas a acoso.

Conducir la sesión:

Parte 1 - ¿Por qué la documentación es importante?
1. Explica

¿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 cuando estés intentando 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 un 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.*

Parte 2 – ¿Cómo podemos documentar incidentes?
2. Entrega copias de la siguiente plantilla de "Cuaderno de documentación".

3. Aclara que estas plantillas sólo brindan un ejemplo de los tipos de información que puede ser importante recopilar cuando estás documentando un incidente. Puedes libremente agregar o quitar columnas y campos de la plantilla según vayas creando formatos más específicos que se ajusten a tu contexto de trabajo.

Aquí incluímos dos plantillas: una para documentar incidentes en línea; otro para incidentes físicos/offline (en la siguiente página):

Plantilla de diario de documentación (Online)

Fecha	**Hora**	**Resumen del incidente**	**Platforma**	**URL**	**Captura de pantalla** ***(nombre del archivo o copiar/pegar)***	**Descripción de la captura de pantalla/contenido**	**Nivel de riesgo**	**Pasos de seguimiento**	**Anotaciones**

Plantilla de diario de documentación (offline/físico)

Fecha	**Hora**	**Ubicación**	**Resumen del incidente**	**Personas involucradas**	**Nivel de riesgo**	**Pasos de seguimiento**	**Anotaciones**

4. 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.

5. 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.

Opcional: *ya sea antes o justo después de la sesión, repasa el ejercicio de "**Modelo de riesgos con perspectiva de género**". Durante el ejercicio, el grupo tendrá una oportunidad de enfocarse en definir niveles de riesgo para su propio contexto. Pueden aplicar estas definiciones de riesgo en su cuaderno de documentación.*

. En último lugar, otro campo a destacar es "Pasos de seguimiento". Básicamente, un paso de seguimiento es lo siguiente que se va a abordar ante el incidente actual (por ejemplo, reportarlo en Facebook) o una medida que se va a implementar para prevenir que el incidente se repita o reducir su impacto.
Opcional: *ya sea antes o justo después de la sesión, repasa la sesión "Planes y protocolos de seguridad en organizaciones". Durante el ejercicio, el grupo tendrá una oportunidad de enfocarse en definir planes y protocolos de seguridad en respuesta a cierto tipo de riesgo conocido o potencial.*

Parte 3 – Empezar nuestro cuaderno de documentación
7. 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.

8. Una vez que hayan terminado la versión borrador de su cuaderno, las participantes se juntan en parejas y comparten los incidentes que documentaron. Tiene sentido que personas de la misma organización se junten en este paso para intercambiar impresiones sobre sucesos vividos por la organización. Cada persona formula preguntas a su pareja sobre el nivel de detalle y rigor de sus reportes. En algunos casos, ésto puede ayudar a la participante a recordar detalles específicos que quizás haya olvidado. **Quizás algunas no se sientan cómodas compartiendo su cuaderno con las demás.** En estos casos, déjales la opción de trabajar individualmente.

Parte 4 - Prácticas y consejos para mantener un cuaderno de documentación
9. Recuerda a las participantes que, para sostener la práctica de documentar en nuestro cuaderno, necesitaremos encontrar maneras para "socializar" o "integrar" su actualización en las rutinas cotidianas que llevamos a cabo. En el contexto de una organización, piensa si habrá una persona encargada de recopilar la información; quizás sea más fácil o más consensuado rotar esta tarea entre las personas del grupo o entre diferentes comisiones. Es recomendable que también comentes aquí que puede ser buena idea, si alguien adentro de la organización es el blanco del incidente, que otra persona sea quien lo documente.

10. Anima a las participantes a probar diferentes flujos de trabajo para encontrar maneras más eficientes de actualizar el cuaderno. Puede ser que encuentren formas de automatizar ciertas partes del proceso o puede ser que omitan ciertos campos de las plantillas que sean irrelevantes para su contexto.

11. Cierra la sesión preguntando a las participantes, ahora que han tenido tiempo para reflexionar sobre la importancia de documentar los incidentes que suceden en sus propios contextos, si sacan conclusiones clave de esta discusión o ideas para alimentar sus cuadernos.

Hagamos doxxing al troll

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.

Objetivo(s): 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.

Módulo Violencia en línea contra las mujeres

Duración: 3 horas

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa.
- Navegación más segura (Activismo online más seguro)
- ¿Qué dice tus metados sobre ti? (Activismo online más seguro)

Ejercicios y sesiones relacionadas:

- Navegación más segura (Activismo online más seguro)
- ¿Qué dice tus metados sobre ti? (Activismo online más seguro)
- ¡Empecemos a crear un diario de documentación! (Violencia en línea contra las mujeres)

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.

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:

> *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**	**Resunen del incidente**	**Platforma**	**URL**	**Captura de pantalla** *(nombre de 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 StartPage (https://startpage.com) o DuckDuckGo (https://duckduckgo.com).

- Recomienda usar **Tails** (https://tails.boum.org) o cuando no sea posible, usar el **navegador Tor** (https://www.torproject.org).

- Búsqueda avanzada en **Twitter** (https://twitter.com/search-advanced).

- Checa **Whois.net** para buscar información vinculada a un sitio web como quién es propietario/a del dominio.

- **Búsqueda inversa de imágenes en Google** (https://images.google.com/) para rastrear imágenes y fotos que hayas podido recibir.

- **Herramientas de metadatos** en caso de que hayas recibido imágenes o fotos:

    - **MetaShield** (https://www.elevenpaths.com/technology/metashield/index.html)
    - **MetaPicz** (http://metapicz.com)

- **Social Mention** ("Mención social") (http://socialmention.com);

- **Follower Wonk** (https://moz.com/followerwonk);

- **NameCheck** ("Verificar nombres") (https://namechk.com);

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.

- **IFTTT** (https://ifttt.com) – 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 Alerts** (https://www.google.com/alerts)
- **Tweetdeck** (https://tweetdeck.twitter.com)

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
- 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

Sexting

Participar de manera más segura en un acto placentero de resistencia contra el racismo, sexismo, machismo, conservadurismo y heteronormatividad.

¡Empieza la función!

Objetivo(s): introducir la práctica de "sexting" desde una perspectiva de género, con énfasis en cómo la violencia sigue siendo violencia independientemente si se ejerce online u offline.

Módulo: Sexting

Duración: 15 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

Ninguno requerido

Sesiones y ejercicios relacionados:

Ninguno

Materiales requeridos:

- Computadora y proyector configurados
- Altavoces/parlantes (para vídeo)

Conducir la sesión:

Carga la página *https://vimeo.com/cyberwomen/1* y selecciona el vídeo “Caso 1”. Muéstralo a las participantes. Facilita una discusión grupal sobre lo que vieron en el vídeo. ¿Qué piensan sobre la situación que retrata? ¿Qué harían ellas?

Referencias:

- **https://acoso.online**

Sexting

Objetivo(s): continuar la discusión sobre sexting desde una perspectiva de género planteada en la sesión anterior "¡Empieza la función!" de este módulo. Conoceremos prácticas y herramientas para un sexting más seguro.

Módulo: Sexting

Duración: 40 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- ¡Empieza la función! (Sexting)
- ¿Qué dicen tus metadatos sobre ti? (Activismo online más seguro)
- Anonimato (Anonimato)
- Introducción al cifrado (Cifrado)

Sesiones y ejercicios relacionados:

- Tus derechos, tu tecnología (Repensando nuestra relación con las tecnologías)
- ¡Empieza la función! (Sexting)
- ¿Qué dicen tus metadatos sobre ti? (Activismo online más seguro)
- Anonimato (Anonimato)
- Introducción al cifrado (Cifrado)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Altavoces/Bocinas

Conducir la sesión:

Parte 1 - ¡Desentrañar el estigma social!

1. Arranca mostrando algunos ejemplos de campañas contra el sexting. Pueden ser videos, carteles, anuncios que contengan narrativas de "prevención de sexting" o "razones de por qué es malo el sexting".
2. Divide las participantes en grupos pequeños de 3-4 para analizar las campañas. Tienen 10 minutos para discutir:

- ¿Qué tienen de malo estas campañas?
- ¿Cómo retratan a las mujeres?
- Algunas campañas hasta criminalizan el sexting y las mujeres que lo practican. ¿Crees que este abordaje realmente es una solución al "problema"?

Parte 2 - ¿Qué es sexting?

3. Revisa con las participantes qué es el sexting, reforzando los siguientes puntos:

- *La práctica de tomar y enviar selfies y desnudos puede ser un acto de auto-determinación.*
- *El sexting puede ser un acto placentero de resistencia contra el racismo, sexismo, machismo, conservadurismo y heteronormatividad.*
- *En última instancia, que compartas o no ese tipo de fotos de ti misma es tu, y solo tu, decisión: un ejercicio consciente de tu derecho a auto-expresarte y tu derecho a la privacidad.*

Parte 3 – ¿Sexting más seguro?

4. Comparte algunas recomendaciones específicas de prácticas que pueden implementar las participantes para hacer sexting de manera más segura. Es importante recordar que existen diferentes actitudes con respecto al manejo de identidades y anonimato en el sexting: algunas personas pueden sentirse más cómodas haciendo sexting con personas que no conocen; otras pueden sentirse más seguras con personas que conocen bien.

Es importante estar abiertas a cualquier posibilidad. Ofrece consejos y recomendaciones de seguridad digital basándote en las preferencias y dudas específicas compartidas por las participantes. Puedes apoyarte en las siguientes sugerencias:

- ***Juego seguro*** *- elimina los desnudos y selfies que mandas justo después de enviarlos. Utiliza canales seguros (como Signal - véase paso 5)*
- ***Construye acuerdos/reglas*** *con la contra-parte sobre compartir fotos, qué tipo de detalles puede contener la foto, cómo enviarán las fotos, etc.*

- ***Usa un canal o app dedicado sólo a sexting.*** *Aunque pueda parecer "poco sexy" pedir a la otra persona descargar una nueva app o seguir un procedimiento específico antes de empezar a hacer sexting, es mejor tomar precaución para evitar enviar la foto a otra persona.*
- ***Creatividad -*** *busca ángulos seguros y sexies para tomarte fotos.*

5. Si no han llevado a cabo la sesión ¿Qué dicen tus metadatos sobre ti? (o no tendrás tiempo de hacerlo en el taller/ciclo de sesiones), dedica 15 minutos durante la sesión a explicar qué son los metadatos y comparte algunos ejemplos. Puedes basarte en la sesión "¿Qué dicen tus metadatos sobre ti?" para tomar ejemplos.

Explica que los metadatos de las imágenes suelen proporcionar información que nos pueden identificar, lo que es especialmente importante en caso de mandar desnudos y querer mantener nuestro anonimato.

- *Si quieres ser anónima, evita sacarte fotos donde aparezcan elementos que te puedan identificar: rasgos obvios (tu cara, nombre de usuaria), detalles (tatuajes, muebles o pertenencias que aparezcan a tu alrededor en segundo plano, determinadas prendas) y rastros digitales (metadatos, etiquetas de ubicación, información sobre el dispositivo).*

6. Finalmente, puedes dar un cierre a la sesión haciendo recomendaciones sobre determinadas herramientas:

- **ObscuraCam:** app celular desarrollada por tThe Guardian Project que permite "limpiar" (eliminar) determinados metadatos de nuestras fotos.

- **Meet.jitsi:** plataforma web que ofrece cifrado HTTPS y permite que las usuarias crear salas temporales para chat de voz y video.
-
- **Signal o Telegram:** apps de mensajería instantánea (chat) que ofrece diferentes niveles de protección de cifrado (del envío/tránsito de datos entre usuarias), además de permitir verificar usuarias. Esto quiere decir, que tiene mecanismos técnicos para garantizar que la persona con la que te comunicas es quien dice ser.
-
- Signal o Telegram te permiten establecer una "caducidad" a los mensajes y otros contenidos que envías (por ejemplo, después de 1 de enviarla, la foto es borrada automáticamente.)

Referencias:

- https://www.codingrights.org/pt/manda-nudes
- http://seguridadigital.org/post/148199830243/sextea-con-seguridad-diagrama

- http://lucysombra.org/TXT/Fanzine_necesito_privacidad.pdf
- https://guardianproject.info/apps/obscuracam
- https://meet.jit.si
- https://signal.org
- https://telegram.org
- https://acoso.online

Buscando la mejor solución

Las herramientas no son remedios milagrosos. La reflexión crítica y tomar decisiones con fundamento son los pilares de una seguridad digital holística y robusta.

Modelo de amenazas con perspectiva de género

Sesión basada en la actividad desarrollada por Jennifer Schuite para el Gender Retreat (Retiro de Género) en Berlín (Alemania) y también basada en el "Manual de Gestión de Riesgos de Desastre para Comunicadores Sociales" (UNESCO).

Objetivo(s): identificar riesgos específicos que enfrentamos como mujeres y defensoras; diseñar estrategias de seguridad que aborden dichos riesgos.

Módulo: Buscando la mejor solución

Duración: 40-50 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Varias (véase "Recomendaciones" a continuación)

Sesiones y ejercicios relacionados:

- ¡Empecemos a crear un diario de documentación! (Violencia en línea contra las mujeres)
- Planes y protocolos de seguridad en organizaciones (Planeando con anticipación)

Materiales requeridos:

- Material de papelería
- Marcadores de colores
- Rotafolio o pizarrón

Recomendaciones:

- Esta sesión se puede facilitar de varias maneras:

    - Conducir la sesión entera al comienzo de la capacitación y retomar la parte 3 de esta sesión una vez que ya hayan repasado herramientas y prácticas más específicas.

- Divide la sesión en 3 mini sesiones. La primera la puedes llevar a cabo al principio de la capacitación, la parte 2 hacia la mitad de la capacitación, una vez que las participantes hayan tenido la oportunidad de discutir sobre seguridad digital en sus contextos personales; y la parte 3 hacia el final cuando ya hayan repasado prácticas y herramientas más específicas;

- Esta sesión puede aplicarse tanto a contextos personales como organizacionales, lo cual es útil en la medida que las participantes también forman parte de grupos de este tipo.

- Esta sesión entraña una discusión en profundidad sobre riesgos personales desde una mirada contextualizada de defensoras de derechos humanos, especialmente la parte 3 (sobre todo si se lleva a cabo toda esta sesión de manera íntegra). Puede detonar desconcierto y estrés entre las participantes por lo que es extremadamente importante que, como facilitadora, manejes los niveles de estrés en la sala. Procura de vez en cuando recordar al grupo que esta sesión está enfocada en última instancia, a identificar estrategias, herramientas, redes y aliadas que nos puedan ayudara afrontar riesgos; no quieres que sientan miedo. Hay muchas acciones que pueden emprender para abordar la violencia en línea.

Conducir la sesión:

Parte 1 – Identificar riesgos & probabilidades

1. Arranca la sesión discutiendo en grupo sobre los riesgos específicos que las defensoras enfrentan, o potencialmente enfrentan. Repasa que el concepto "riesgo" significa la posibilidad de que ocurra un daño o evento nocivo. Anota algunos ejemplos específicos compartidos por las participantes. Repásalas después de haber recopilado lo que consideres una muestra relevante.

2. Facilita la discusión buscando abordar el carácter dinámico de los riesgos. La **probabilida**d de un riesgo fluctúa dependiendo del número de factores externos como:

- El riesgo de que una persona adversaria intercepte un mensaje de texto aumenta cuando se usa una app regular de SMS vs. utilizar una app que cifra los datos como Signal.

- Si alguien es una activista "fichada" en su país, es mucho más probable que sus comunicaciones sean interceptadas, especialmente si usa un app normal y corriente de SMS y las envía por un proveedor de telefonía celular de su país. Si usa una app como Signal y/o se conecta a un proveedor internacional, la probabilidad del riesgo disminuye considerablemente.

El ejemplo anterior retrata cómo factores técnicos externos influyen en la probabilidad de un riesgo. Y el género, ¿es un factor de riesgo? ¿Las defensoras enfrentan los riesgos de la misma manera que sus compañeros varones?

3. Dibuja una tabla como la que incluimos a continuación en un papel grande. Enumera una serie de riesgos digitales en la columna correspondiente. Puedes basarte en los ejemplos compartidos y discutidos en el paso 1. Asegúrate de dejar espacio a la derecha de esta columna por si se quieren agregar campos extra después.

Riesgo digital	**Probabilidad**

4. Ahora identifiquen, para cada riesgo, la probabilidad de que suceda, lo que quizás sea más fácil si los contextos de vida del grupo sean comunes y afines (viven en el mismo país, tipo de activismo, etc.). En caso de que las trayectorias sean muy diversas, quizás quieran trabajar partiendo del contexto de un "personaje hipotético".

5. Para medir la probabilidad de cada riesgo, puedes basarte en el siguiente tabla. Por ejemplo, puede ser una escala de 1 a 5, donde 5 sea "probabilidad muy alta".

Rellena la tabla conforme van discutiendo cada riesgo.

Riesgo digital	**Probabilidad** 1= Muy bajo 5= Muy alto
¡Hacer clic, sin querer, en un enlace que contiene malware!	4
¡Nuestras oficinas son allanadas por fuerzas policiales y confiscan nuestros discos duros y otros dispositivos!	2

Parte 2 – Determinando el impacto

6. Ahora determinarán los impactos reales de estos riesgos: cuáles son las consecuencias a nivel individual, organizacional, de red, etc. si un riesgo se hiciera efectivo.

7. Explica que, justamente por la propia naturaleza de los riesgos, los impactos pueden variar bastante. Cómo va a ser un impacto y qué tan grave se vuelve depende de factores externos. ¿Va a tener impacto a un nivel personal u organizacional? Quizás tenga implicaciones en ambas dimensiones y, si fuera así, ¿en qué se parecen y se diferencian estos impactos?

8. Para la siguiente parte de la sesión, crearán un baremo para medir impacto. Puede ser cuantitativo (numérico) parecido al que utilizamos para medir la probabilidad de cada riesgo o puede ser cualitativo (descriptivo) en el que den más detalle sobre la naturaleza del impacto. Ustedes escogen. Lo que importa es que se centren en determinados riesgos y consecuencias de tal manera que las participantes entiendan estas situaciones de manera más empírica (y no sólo como conceptos abstractos).

9. Explica al grupo que una parte importante de comprender y dimensionar un riesgo tiene que ver con anticipar cómo podríamos reaccionar ante su impacto. Pregúntale a las participantes cómo creen que se comportarían, a nivel personal, ante un determinado riesgo. Después, discutan, al igual que hicieron al analizar las probabilidades e impactos de los riesgos, cómo crearán un baremo para medir las reacciones. Esta escala, de nuevo, puede ser cualitativa o cuantitativa. En el ejemplo que exponemos, usaremos una escala cuantitativa.

Riesgo digital	**Probabilidad** 1= Muy bajo 5= Muy alto	**Impacto** 1= Gravedad/severidad/ intensidad baja 5=Gravedad/severidad/intensidad alta	**Reacción** 1= Tranquilo, bajo control 5= Pánico, alto estrés
¡Accidentalmente hacer clic en un enlace que contiene malware!	4	3	3

¡Nuestras oficinas son allanadas por fuerzas policiales y confiscan nuestros discos duros y otros dispositivos!	2	5	5

Parte 3 – Creando estrategias de respuesta

10. Como comentamos en "Recomendaciones", esta sesión entraña una discusión en profundidad sobre riesgos personales desde el contexto de las defensoras de derechos humanos. Es probable que detone desconcierto y estrés entre las participantes. En la siguiente parte de la sesión, se enfocarán en identificar estrategias, herramientas, redes y aliadas que nos puedan ayudar a afrontar riesgos. No quieres infundir miedo sino todo lo contrario: hay muchas acciones que podemos emprender para combatir la violencia en línea.

11. Ahora que ya identificaron y dimensionaron las probabilidades, impactos y reacciones ante determinados riesgos, explica que ahora abordarán respuestas y soluciones. Para cada riesgo, pregúntale a las participantes: ¿qué puedes hacer para abordar un riesgo y/o prevenirlo? Las respuestas que brindarán dependerá de qué cosas cubrieron anteriormente en la capacitación. Si están hacia el comienzo, quizás no compartan respuestas muy en detalle. Si están llegando al final de las sesiones, van a plantear aportaciones más específicas y relacionadas con determinadas prácticas y herramientas.

12. Volviendo a la tabla que han estado trabajando en esta sesión, crea una columna nueva que diga "¿Qué podemos hacer?". En ella, escribe las respuestas compartidas en el grupo. Cuelga esta tabla en un lugar visible de la sala para que puedan volver a ella más en adelante para re-leer y analizar respuestas. Así las participantes podrán determinar después si hace falta agregar algo más a la tabla, referencia que después pueda ser un punto de partida para diseñar protocolos de seguridad digital.

La tabla podría parecerse a algo como lo siguiente:

Riesgo digital	**Probabilidad** 1= Muy bajo 5= Muy alto	**Impacto** 1=Gravedad/severidad/ intensidad baja 5= Gravedad/severidad/ intensidad alta	**Reacción** 1= Tranquilo, bajo control 5= Pánico, alto estrés	**¿Qué puedo hacer?**
¡Accidentalmente abrir un link de un correo que recibí que contiene malware!	3	4	3	Descargar e instalar un software de antivirus; avisar a las demás personas de mi red/organización en caso de que se encuentren con el mismo enlace.
¡Nuestras oficinas son allanadas por fuerzas policiales, confiscaron nuestros discos duros y otros dispositivos!	4	5	5	Realizar respaldos frecuentes de nuestros datos, almacenarlos en un lugar seguro fuera de la oficina, avisar a las demás personas de nuestras redes si se compromete información que les concierne.

Referencias:

- https://ssd.eff.org/es/module/evaluando-tus-riesgos

Toma de decisiones sobre seguridad digital

Objetivo(s): introducir el proceso de pensamiento crítico estratégico necesario para tomar decisiones fundamentadas a la hora de implementar prácticas y herramientas de seguridad digital. Identificar recursos que puede ayudarlas a mantenerse al día después de la capacitación.

Módulo: Buscando la mejor solución

Duración: 90 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Conceptos básicos de seguridad digital y/o capacitación previa;

Sesiones y ejercicios relacionados:

- Impresiones personales sobre la seguridad (Repensando nuestra relación con las tecnologías)
- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- ¿Cómo funciona Internet? (Conceptos básicos de seguridad digital | Parte 1)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a? (Privacidad)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados
- Copias impresas de infográficos de casos de defensoras (Véase Apéndice)

Recomendaciones:

- Puesto que esta sesión requiere un nivel básico de conocimiento de partida sobre conceptos de seguridad digital, es ideal llevarla a cabo en el contexto de una capacitación de varios días o parte de un taller corto que se centra en diseñar protocolos individuales de seguridad.

Conducir la sesión:

Parte 1 - Introducción

1. Arranca preguntándole a las participantes cuántas veces han preguntado a un tallerista, facilitadora o experta algo sobre seguridad digital y les han respondido de manera diferente cada vez. Un poco confuso, ¿verdad? A veces, cuando pedimos consejo sobre seguridad digital, no necesariamente implica que nos vayan a acompañar en el proceso sino sólo "arreglar el problema" en nuestros dispositivos sin explicarnos lo que hicieron. ¿Preferirías saber para poder replicar el proceso después si vuelve a surgir el problema?

2. El objetivo de esta sesión es introducir el proceso de pensamiento crítico estratégico necesario para tomar decisiones fundamentadas a la hora de implementar prácticas y herramientas de seguridad digital e identificar recursos que nos pueden ayudar a mantenernos al día después de la capacitación. Conversen sobre cómo la seguridad digital es más que descargar unas apps nuevas sino que es un proceso de conocer nuestras prácticas más de cerca y tomar decisiones con fundamento con el fin de construir entornos más seguros para nosotras mismas.

Parte 2 – ¿Cómo desarrollaron el software que utilizas?

3. Muestra de nuevo herramientas y plataformas que quizás ya hayas presentado como Signal, HTTPS Everywhere, ObscuraCam, Skype, Telegram, etc. Identifiquen qué tipo de software es en cada caso. Pueden entrar en los sitios web para obtener más contexto.

4. Explica qué es el **software propietario** (código cerrado): ¿cuáles son las características de este tipo de software? Brinda ejemplos. ¿Cuáles son las implicaciones, a nivel de seguridad digital, al utilizar este tipo de software?

5. Explica qué es el **software open source:** ¿cuáles son las características de este tipo de software? Brinda ejemplos. ¿Cuáles son las implicaciones, a nivel de seguridad digital, al utilizar este tipo de software? Asegúrate de introducir qué es la comunidad de software opensource y la auditoría de código.

6. Explica qué significa **FLOSS (Free/Libre and Open Source Software)** : ¿cuáles son las características de este tipo de software? Brinda ejemplos. ¿Cuáles son las implicaciones, a nivel de seguridad digital, al utilizar este tipo de software?

Parte 3 – Tomando en cuenta a las usuarias

7. Si ya cubrieron la sesión **¿En quién confías?** del módulo "Repensando nuestra relación con las tecnologías", repasa ejemplos de adversario/as. Si ya cubrieron la sesión de **Modelo de riesgos con perspectiva de género**, revisa de nuevo el modelo que crearon juntas.

Este repaso sirve para reforzar la idea de que no todo el mundo tiene las mismas necesidades o enfrenta los mismos riesgos en materia de seguridad digital.

- *Cuando estamos buscando respuestas en estos temas, sondea lo máximo posible sobre las necesidades específicas que vayas identificando. ¿Qué quieres hacer o asegurar? ¿Cuál es el lugar más seguro donde guardas algo? ¿De quién lo estás protegiendo?*

- *Piensa en las plataformas y herramientas que utilizas. ¿Qué tan dispuesta o qué tan posible es para ti cambiarlas por otras alternativas o cambiar tu manera en que interactúas con ellas?*

- *¿Hasta qué punto te afecta tu acceso a internet a la hora de crear posibles respuestas de seguridad digital? ¿Sueles tener una conexión estable y confiable de internet o te tienes que adaptar a trabajar sin conectividad durante largos periodos de tiempo?*

- *Si estás considerando crear estrategias de seguridad digital para una organización o colectivo, toma en cuenta los diferentes dispositivos y sistemas operativos que las personas en el grupo están utilizando. ¿La estrategia va a poder aplicarse a todo el mundo? ¿O para la mayoría?*

Parte 4 – Pensando en herramientas

8. Las siguientes preguntas son importantes a la hora de considerar nuevas plataformas o herramientas. No tienes que repasarlas ni contestarlas todas (ya que son muy específicas), pero procura leerlas en voz alta y dar un poco de contexto de por qué son relevantes:

- *¿Es software libre o open source?*
- *¿Conoces quién lo desarrolló y/o financió?*
- *¿Está disponible en mi idioma?*
- *Busca referencias en internet. ¿Qué información encontraste?*
- *¿Cuándo fue actualizado por última vez?*
- *¿Existe una versión estable disponible?*
- *¿Hay un canal de soporte?*
- *¿Qué tan fácil es de configurar?*
- *¿Ha sido testeado o auditado?*
- *¿Está disponible para tu sistema operativo?*
- *Verifica los Términos de Servicio. ¿Estás de acuerdo con ellos o hay algo que te levanta sospecha?*
- *Si la herramienta o plataforma utiliza servidores remotos, ¿sabes dónde están ubicados?*

- *¿Sabes si las personas desarrolladoras han entregado datos de usuarias ante una petición de una entidad gubernamental?*
- *¿Cómo almacenan la información en sus servidores? ¿Está cifrada? ¿Las personas del proyecto pueden descifrar y acceder a la información?*

9. Subraya de nuevo que no existe una respuesta o recomendación universal en materia de seguridad digital. Ninguna herramienta se adapta al contexto de todas. Ser estratégica a la hora de manejar herramientas y prácticas de seguridad digital tiene más que ver con conocernos mejor como usuarias y, a partir de ahí, escoger herramientas que se ajustan mejor a nuestros conocimientos y circunstancias.

10. Señala que existe mucho software de seguridad digital que implementa el cifrado en diferentes niveles. Explica la relevancia de que este tipo de software sea open source (es decir, que su código sea disponible). El software open source puede ser revisado por la comunidad para asegurar que no tiene puertas traseras; si no es una prioridad para ti que implemente cifrado, entonces puede ser que este criterio sea menos relevante (aunque puede ser ventajoso de todas maneras, por ejemplo, en términos monetarios).

11. Las participantes se dividen en grupos de 3-4 personas (máximo) y hacen una lista de todas las herramientas de seguridad digital que conocen. Responderán a las preguntas del punto 8. Cada grupo tiene 10 a 15 minutos para discutir las ventajas y desventajas de cada herramienta enumerada. Al final, compartirán lo reflexionado al resto de los grupos.

Parte 5 – Practicar a pensar en respuestas

12. Distribuye a los grupos los infográficos de casos de defensoras de derechos humanos (véase Apéndice). Asegúrate, antes de la sesión, tener suficientes para repartir. No les reveles posibles soluciones ahora. La idea es que los grupos piensen por su cuenta cuáles son posibles respuestas que se pueden llevar a cabo basándose en lo que llevan aprendido hasta ahora.

Parte 6 – Materiales para mantenerse al día

13. Es importante que las participantes tengan acceso a materiales complementarios después de la capacitación para que puedan remitir a ellos y mantenerse al día con herramientas y prácticas de seguridad digital.

Aquí recomendamos algunos:

- **Zen y el arte de que la tecnología trabaje para ti (Tactical Technology Collective)** https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es

- **Security in a Box** (Frontline Defenders & Tactical Technology Collective)

https://securityinabox.org/es

- **Autoprotección Digital Contra La Vigilancia** (Electronic Frontier Foundation) https://ssd.eff.org/es/module/eligiendo-tus-herramientas

- **Genios de Internet (Español) (**Karisma Foundation) https://karisma.org.co/genios-de-internet-una-guia-para-mejorar-tu-seguridad-en-la-red

Opcional*: pueden listar diferentes organizaciones que siguen (online, en Twitter, etc.) para obtener información sobre seguridad digital en contextos locales.*

Referencias:

https://www.seguridad.unam.mx

Yo decido

Objetivo(s): realizar juntas un proceso de pensamiento crítico estratégico con el fin de tomar decisiones sobre prácticas y herramientas de seguridad digital que van a implementar para ellas mismas.
Módulo: Buscando la mejor solución

Duración: 15 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:
- Práctica con herramientas y prácticas de seguridad digital
- Decisiones sobre seguridad digital (Buscando la mejor solución)

Sesiones y ejercicios relacionados:
- Impresiones personales sobre la seguridad (Repensando nuestra relación con las tecnologías)
- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- ¿Cómo funciona Internet? (Conceptos básicos de seguridad digital | Parte 1)
- Apps & Plataformas online: ¿Amigo/a o enemigo/a? (Privacidad)
- Digital Security Decisions (Buscando la mejor solución)

Materiales requeridos:
- Fichas de seguridad digital (idealmente 2-3 copias de cada para repartir; no hace falta que haya una por persona)

Recomendaciones:
- Como facilitadoras, podemos caer en imponer nuestra perspectiva, ya sea conscientemente con "buenas intenciones" o incluso sin darnos cuenta. Sin embargo, es importante mantener en mente que el grupo no tiene la obligación de implementar las herramientas y prácticas que estamos explicando.

Conducir la sesión:

1. Arranca la sesión explicando cómo las prácticas de seguridad digital son procesos iterativos y generalmente difíciles para todas. Esta sesión se basa en la de "Decisiones de seguridad digital" de este mismo módulo, en la que las participantes empezaron a reflexionar juntas e identificar necesidades. Ahora te pondrás a trabajar con las participantes a identificar herramientas y prácticas específicas para que apliquen en sus vidas.

2. Sobre una mesa o superficie plana - en medio de la sala o en un sitio visible para todas- coloca las fichas de seguridad digital.

3. Seguramente reconozcan muchas de las herramientas mencionadas, como por ejemplo llaves PGP, Signal, ObscuraCam, HTTPS Everywhere, etc. Enfatiza que son ellas las que van a escoger las herramientas que se ajustan más a sus contextos y necesidades. Nadie más va a decidir sobre ellas: ni una persona facilitadora, ni una persona técnica, ni nadie más.

4. Cada participante seleccionará las fichas de herramientas que sean relevantes para ellas y que planean implementar después del taller.

5. El grupo se sienta en círculo y cada una compartirá al resto del grupo por qué escogieron las herramientas que escogieron. También pueden comentar si hay otras herramientas que quieren seguir practicando aunque no lograron tomar la ficha de ella.

6. Pregúntales si echan en falta otras herramientas, aunque no se sepan el nombre concreto o no exista. Sondea si hay dudas o inquietudes y abórdalas.

7. Cierra la sesión reflexionando juntas sobre cómo se comparte el conocimiento y cómo pueden socializar sus procesos de aprendizaje de seguridad digital entre ellas.

Planeando con anticipación

¿Qué sigue? Cómo pueden mantener constancia las organizaciones a la hora de implementar prácticas colectivas de seguridad digital.

Planes y protocolos de seguridad en organizaciones

Objetivo(s): desarrollar un plan y protocolos de seguridad para implementar medidas de seguridad digital en su propia organización.

Módulo: Planeando con anticipación

Duración: 90 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Familiaridad con herramientas y prácticas de seguridad digital
- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

Sesiones y ejercicios relacionados:

- Impresiones personales sobre la seguridad (Repensando nuestra relación con las tecnologías)
- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- ¿Cómo funciona Internet? (Conceptos básicos de seguridad digital | Parte 1)
- Modelo de riesgos con perspectiva de género (Buscando la mejor solución)
- Planes y protocolos de seguridad digital: replicar después del taller (Planeando con anticipación)

Materiales requeridos:

- Modelo de riesgos del ejercicio "Modelo de riesgos con perspectiva de género"
- Plantillas impresas de protocolos de seguridad (véase plantilla a continuación)

Recomendaciones:

- Esta sesión se dirige especialmente a participantes que estén en la misma organización o colectiva ya que la intención es enfocarse en desarrollar protocolos de seguridad digital a nivel organizacional. El proceso de co-diseñar ésto juntas facilitará el proceso de implementación.

- Es fundamental dar un seguimiento a la implementación del plan creado en esta sesión. Si es posible, vuelve a contactar con ellas 2 o 3 semanas después para saber cómo van, aparte de mantener comunicación por correo para resolver preguntas, Presta atención en no presionarlas a utilizar determinadas herramientas o implementaciones durante el seguimiento. Estás ahí para darles apoyo, presentarles opciones y responder a preguntas e inquietudes durante el proceso. Si las participantes se sienten presionadas, puede obstaculizar la comunicación.

Conducir la sesión:

Parte 1 – Volver al Modelo de Riesgos

1. Comienza la sesión subrayando la importancia de construir un modelo de riesgos antes de diseñar un plan y protocolos. La seguridad digital es, ante todo, un proceso personal. Si el objetivo es esbozar e implementar un plan de seguridad digital a un nivel organizacional, explícales que ese proceso implica:

- Mapear colectivamente amenazas. Ésto se puede hacer a lo largo de las sesiones con el equipo entero presente, pero siempre tomando en cuenta que van a tener que ir actualizando este modelo a lo largo del tiempo.

- Aprender la diferencia entre qué hábitos nuestros, en la dimensión digital, generan resiliencia y cuáles detonan inseguridad. También aprenderemos a dar mantenimiento a las herramientas que ya utilizamos y estar al día en nuevas herramientas y prácticas que podemos ir incorporando.

- Tomar decisiones en grupo sobre qué y cómo vamos a implementar colectivamente, a la vez que identificar áreas donde cada persona puede crear y llevar a cabo sus propios procesos como vayan viendo necesario.

- Monitorear de manera consistente la implementación de nuestro plan de seguridad digital organizacional, asegurándonos que los protocolos acordados son entendidos por todo el grupo antes de llevarlas a cabo. También es importante sondear cuáles son las dificultades que van surgiendo en el proceso.

Parte 2 – Planes vs. Protocolos

2. Explica la diferente entre un plan de seguridad digital y un protocolo. La idea principal a transmitir es:

- Un **plan** es un esbozo de cambios fundamentales que una organización o colectivo identifica como necesarios para fortalecer su seguridad digital. Los planes se definen como procesos, con un principio y fin.

- Un **protocolo** es una serie de medidas o acciones relacionadas con la seguridad digital que se asocian a actividades o procesos específicos dentro de una organización o colectivo. Los protocolos son procesos que persisten más allá de la implementación de un plan de seguridad digital. Evolucionan a lo largo del tiempo en respuesta a los cambios en nuestros entornos de riesgos y amenazas.

Brinda ejemplos de planes y protocolos, por ejemplo, actividades como viajar o participar en manifestaciones públicas implican su propio protocolo de seguridad digital; algunos componentes de un plan de seguridad digital pueden ser la auditoría de un sitio web, verificar que todos los dispositivos tengan un antivirus e introducir el uso de PGP para cifrar comunicaciones por mail.

Parte 3 - Crear un plan y protocolo organizacional

3. Esta sesión está enfocada especialmente a participantes que estén en la misma organización o colectiva ya que la intención es enfocarse en desarrollar un plan y protocolos de seguridad digital a nivel organizacional. Sin embargo, si hay participantes que no están en una organización o colectivo, también pueden participar en la sesión diseñando sus propios planes y protocolos.

4. Se basarán en el modelo de riesgos que crearon en la sesión de "Modelo de riesgos con perspectiva de género" y las anotaciones de la sesión de "¿En quién confías?". Primero crearán un borrador de su plan de seguridad. Pueden basarse en el siguiente formato si quieren. Explica cada sección (para cada riesgo o amenaza identificada, crea una nueva fila).

Amenazas y riesgos	**Vulnerabilidades identificadas**	**Fortalezas y capacidades**	**Mitigar acciones**	**Recursos requeridos**	**¿Quién tiene que estar involucrada?**
¿Qué amenazas y riesgos estamos enfrentando en la actualidad? ¿Cuáles vamos a encarar potencialmente en el futuro?	*¿Qué prácticas individuales o circunstancias dentro de una organización pueden exponernos a algun daño?*	*¿Qué fortalezas tenemos como organización frente a amenazas y riesgos identificados?*	*¿Qué medidas tenemos que tomar para mitigar riesgos identificados? ¿Qué podemos hacer para estar más preparadas?*	*¿Qué recursos (económicos, humanos, etc.) necesitamos para implementar estas acciones?*	*¿Qué áreas o personas dentro de nuestra organización necesitamos que estén involucradas en la implementación? ¿Se necesitará alguna aprobación o permiso de alguien?*

5. Recuerda que, aunque el enfoque de esta capacitación es en la seguridad digital, debemos siempre tomar en cuenta medidas más holísticas. Pídeles a las participantes considerar, mientras esbozan un borrador de sus planes y protocolos de seguridad, qué acciones necesitan llevar a cabo a nivel de seguridad física y auto-cuidado.

6. Ahora crearán una lista con todas las actividades y procesos que llevan a cabo en la organización/colectiva que sienten que requiere de protocolos individuales.

7. Ahora pueden tomar un momento para compartir sus planes, lo que les brinda una oportunidad valiosa para aprender las perspectivas de cada una; sin embargo, recuerda que algunas pueden sentirse incómodas compartiendo sus vulnerabilidades o las de su organización/colectiva. Puedes abordar esta cuestión de una manera pro-activa: pide al grupo compartir sólo elementos clave de su plan (la cuarta columna de la tabla "mitigando acciones") y no otra información más confidencial como "amenazas y riesgos" o "vulnerabilidades identificadas".

Parte 4 – ¿Qué sigue?

8. Discute con las participantes los pasos que siguen: tendrán que organizar una reunión dentro de su organización como compartir lo que trabajaron en esta sesión y la del Modelo de Riesgos y "En quién confías". Tendrán que discutir y acordar con sus equipos los planes de seguridad digital que desarrollaron, pensando juntas en un cronograma realista para la implementación. Tengan en cuenta que algunas personas de su organización van a necesitar capacitación en prácticas de seguridad digital y/o herramientas específicas.

Referencias:

- *https://ssd.eff.org/es/module/evaluando-tus-riesgos*
- https://gendersec.tacticaltech.org/wiki/index.php/Diagn%C3%B3sticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitadores

Planes y protocolos de seguridad digital: replicar después del taller

Objetivo(s): seguir construyendo a partir de la sesión de "Planes y protocolos de seguridad en organizaciones". Presentarás una serie de recomendaciones que ayudará a las participantes en la implementación de sus planes y protocolos de seguridad digital después del taller.

Módulo: Planeando con anticipación

Duración: 40 minutos

Formato: Sesión

Nivel de habilidades: Intermedio

Conocimientos requeridos:

- Práctica con herramientas de seguridad digital
- Planes y protocolos de seguridad en organizaciones (Planeando con anticipación)
- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

Sesiones y ejercicios relacionados:

- Planes y protocolos de seguridad en organizaciones (Planeando con anticipación)
- ¿En quién confías? (Ejercicios para fortalecer la confianza)
- Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

Materiales requeridos:

- Diapositivas (con los puntos claves descritos a continuación)
- Computadora y proyector configurados

Conducir la sesión:

Parte 1 – Mapeando estructuras y obstáculos organizacionales

1. 1. Trabaja en parejas. Cada persona describe la organización(es) en la que participa:
    - ¿Cuánta gente hay en ella(s)?
    - ¿Con qué frecuencia se juntan?
    - ¿Existen áreas o comités que integran las diferentes partes de la organización?

2. Las parejas comparten entre si algunos de los obstáculos y retos que anticipan que van a enfrentar en su organización o grupo al presentar sus planes de seguridad digital y articular la necesidad de implementarlas.

Parte 2 – Facilitar el proceso de implementación

3. Comparte algunas ideas que puedan ayudar a las participantes a implementar sus planes y protocolos de seguridad en sus organizaciones y grupos.

- Enmarca esto como el comienzo de un proceso de reflexión. Implementar el plan, además de desarrollar y poner a prueba los protocolos, tomará tiempo. Habrá un periodo de ajuste para que las personas se acostumbren a estos cambios. Independientemente de ello, es mejor que enfaticen que tomar una perspectiva crítica sobre la seguridad de la organización es un paso muy positivo para todas.

- Avisa que puede que haya reticencia con el término "protocolos" ya que pueden considerarlo demasiado técnico e intensivo. Pueden abordar esta reacción explicando que los protocolos no son ni más ni menos que un acuerdo sobre determinados riesgos y amenazas que enfrentan, a la vez que un compromiso de resolverlas juntas a través de estrategias.

- Subraya la importancia de la colaboración e inclusión en el proceso de implementación. Es recomendable que las participantes trabajen con diferentes grupos dentro de sus organizaciones a la hora de hacer el diagnóstico de riesgos para después compartir las reflexiones y siguientes pasos con las demás. Enfatiza también que será crítico crear un espacio de intercambio para que las demás de la organización puedan compartir sus impresiones sobre los planes y protocolos de seguridad digital. Ya que estas nuevas medidas van a afectar a cada una de manera diferente, queremos evitar generar obstáculos y dificultades en su trabajo.

- Consideren otras maneras de hacer partícipes los diferentes grupos dentro de la organización. Pueden crear un comité de "seguridad digital" que incluya representantes de cada grupo o área que tengan el poder de tomar decisiones en el proceso de implementación. También pueden ir abarcando el proceso de manera gradual, incorporando personas dentro de la organización poco a poco. Que lo hagan de una manera u otra depende de cada organización.

- Pide a las participantes compartir algunas ideas de cómo creen que se podría facilitar el proceso de implementación.

Parte 3 – Empezar la conversación

4. Presenta una estructura básica para detonar una conversación dentro de las organizaciones. Puede ser una serie de preguntas o un guión para llevar a cabo una capacitación.

5. Tomen en cuenta la logística que implica cada opción. Puede ser que las personas dentro de la organización o colectiva no tenga tenga suficiente tiempo para apartar una tarde o día entero para un taller. Cambiar hábitos adquiridos toma mucho tiempo y paciencia así que lo ideal sería encontrar maneras de ir construyendo estas conversaciones (o talleres) dentro de los espacios ya existentes (reuniones, encuentros, etc.)

Aquí ponemos un ejemplo de una estructura básica que podrían seguir para generar consciencia sobre ciertos temas. Arranca con una conversación sobre la relevancia de la seguridad digital dentro de una organización. También incluye algunas sesiones de esta currícula que entran más en detalle sobre estos temas. Si van a seguir o no esta estructura o hasta qué punto lo adaptan, depende de cada participante y su contexto:

- **Conversación:** ¿Por qué es tan importante la seguridad digital en tu organización?
- **Sesión:** ¿Cómo funciona Internet? (Conceptos básicos de seguridad digital | Parte 1)
- **Sesión:** ¡Empecemos a crear un diario de documentación! (Violencia en línea contra las mujeres)
- **Sesión:** Celulares | Parte 1 (Celulares más seguros)
- **Sesión:** Comunicaciones cifradas (Cifrado)
- **Sesión:** Navegación más segura (Conceptos básicos de seguridad digital | Parte 1)
- **Ejercicio:** Modelo de riesgos con perspectiva de género (Buscando la mejor solución)

5. Este abordaje es sólo un ejemplo. Siéntate libre de ajustarlo a tu gusto. Hazles saber a las participantes que estás disponible para brindar apoyo en el proceso de implementación de cada una de ellas.

Referencias:

- https://gendersec.tacticaltech.org/wiki/index.php/Diagn%C3%B3sticos_en_seguridad_digital_para_organizaciones_defensoras_de_derechos_humanos_y_del_territorio:_un_manual_para_facilitadores

Auto-cuidado

Nuestro trabajo nunca es fácil. Antes de poder realmente cuidar a las demás personas, primero tenemos que aprender a cuidar de nosotras mismas.

Construyendo un auto-cuidado feminista

Este ejercicio es una adaptación de una parte del manual "Autocuidado y sanación feminista para ingobernables" de Mujeres Al Borde

Objetivo(s): reflexionar juntas sobre la importancia del auto-cuidado en nuestro cotidiano; construir una definición de auto-cuidado en un entorno sin prejuicios.

Módulo: Auto-cuidado

Duración: 30 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Sesiones y ejercicios relacionados:

- Impresiones personales sobre la seguridad (Repensando nuestra relación con las tecnologías)
- ¿En quién confías? (Repensando nuestra relación con las tecnologías)

Materiales requeridos:

- Una pelota de goma (o cualquier objeto pequeño que puedas lanzar)

Recomendaciones:

- El auto-cuidado es una parte esencial de la práctica de seguridad digital holística y es importante reforzarla y alentarla de manera consistente. Recomendamos distribuir los ejercicios de este módulo a lo largo de toda la capacitación.
- Para ésta y las demás sesiones de tu capacitación, procura tomar consciencia y ser sensible a las diferentes capacidades y limitaciones físicas de las participantes.
- Es aconsejable realizar este ejercicio hacia el comienzo de la capacitación. Al ser un ejercicio que implica reflexión e introspección, procura espaciar las demás actividades que tengan una metodología similar.

Conducir la sesión:

1. Arranca el ejercicio introduciendo el concepto de auto-cuidado. Pregúntales a las participantes si están familiarizadas con el concepto y si saben lo que es. Define el concepto de auto-cuidado y explica que en el ejercicio van a centrarse en el auto-cuidado como práctica feminista en el contexto de defensoras de derechos humanos.

2. Presenta la actividad:

- Nos levantamos de nuestros asientos y empezamos a movernos: nos estiramos, andamos por la sala. Nos colocamos todas en círculo.

- Lanzas suavemente una pelota pequeña (o algún objeto que puedas lanzar) a una de las participantes.

- Al atraparlo la compañera, pregúntale qué piensa sobre el auto-cuidado y cómo se vincula con su vida.

- Después de responder, te lanza la pelota de vuelta. La lanzas a otra persona y así sucesivamente. Puedes seguir hasta que todas hayan respondido la pregunta.

Aquí van unos ejemplos de preguntas para el ejercicio. Puedes basarte en ellas o inventarte otras.

- ¿Qué es el auto-cuidado para ti? ¿Qué son los cuidados colectivos? ¿En qué se diferencian?

- ¿Las organizaciones, grupos y/o colectivos en los que estás involucrada abordan este tema?

- ¿Practicas el auto-cuidado? ¿Cuáles son tus prácticas de auto-cuidado?

- ¿Te cuesta pensarte como alguien que merece cuidados?

- Como defensora de derechos humanos, ¿crees que las defensoras tienden a centrarse más en cuidar a los demás a costa de nosotras mismas?
- ¿Sientes que tomas conciencia sobre lo que necesita tu cuerpo y espíritu?

3. Cierra la discusión haciendo un resumen de lo que se compartió en el grupo. ¿El grupo ya estaba, en general, familiarizada con el auto-cuidado como una práctica intencional? Si fuera así, ¿con qué frecuencia la practican? O puede ser que haya diferentes grados de auto-cuidado entre ellas. ¿Qué podemos aprender la una de la otra? Destaca algunas de las aportaciones del grupo y prácticas que llevan a cabo en su día a día. Es bueno reconocer lo que ya hacen en este sentido.

4. Pregunta al grupo: ¿son diferentes las responsabilidades que tenemos como defensoras a las de nuestros compañeros? Conversen sobre las cargas sociales que se espera que lidiemos, especialmente por nuestro rol de cuidadoras, no sólo en nuestras casas y en nuestras familias sino también en otros círculos sociales y nuestro ambiente de trabajo.

5. Analiza cómo estas responsabilidades impactan nuestro trabajo como defensoras y compara nuestra situación a las de nuestros compañeros. También pueden hablar sobre la "culpa" que solemos sentir como defensoras. Muchas veces tenemos que decidir entre nuestro activismo y nuestras vidas personales y que, independientemente de la decisión que tomemos, implica "dejar abajo" a alguien.

6. Cierra el ejercicio intercambiando en el grupo ideas de prácticas de auto-cuidado para esta capacitación. Puede ser empezar más tarde la sesión, tomar más descansos en medio, compartir la hora de la comida, etc.

Referencias:

- http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos/autocuidado

Tacto con amor

Este ejercicio es una adaptación de la guía de autocuidado de IM Defensoras

Objetivo(s): conectarse las unas con las otras a través del tacto y contacto corporal para reflexionar sobre cómo damos y recibimos amor, cariño y afecto.

Módulo: Auto-cuidado

Duración: 20 a 30 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Sesiones y ejercicios relacionados:

- Las Reglas del Juego (Ejercicios para fortalecer la confianza)
- Construyendo un auto-cuidado feminista (Auto-cuidado)

Materiales requeridos:

- Colchones o cobijas
- Almohadas o cojines
- Música relajante en segundo plano.

Recomendaciones:

- El auto-cuidado es una parte esencial de la práctica de seguridad digital holística y es importante reforzarla y alentarla de manera consistente. Recomendamos distribuir los ejercicios de este módulo a lo largo de toda la capacitación.

- Para ésta y las demás sesiones de tu capacitación, procura tomar consciencia y ser sensible a las diferentes capacidades y limitaciones físicas de las participantes.

- Algunas pueden sentirse incómodas ante el contacto físico de las demás (lo que puede variar según el contexto cultural de cada una, por ejemplo). Por ello, es mejor realizar este ejercicio cuando el grupo ya se conoce entre sí y confían las unas en las otras.

- Deja claro que es totalmente aceptable que alguien no quiera participar en el ejercicio. También pueden participar simplemente tumbándose y tomando unos minutos para relajarse, y respirar despacio y profundo.

- Con el fin de crear un entorno que induce a la relajación e introspección, puedes alumbrar unas velas, quemar incienso y/o poner música tranquilizante de fondo durante el ejercicio.

Conducir la sesión:
1. Acomoda las mantas y almohadas en un círculo en el suelo. Pide a la mitad del grupo tumbarse boca arriba, con su cabeza orientada al centro del círculo. Cierran sus ojos y empiezan a relajarse. Asegúrate que haya espacio suficiente entre cada participante.

2. La otra mitad de las participantes se colocan entre sus compañeras que están tumbadas, a nivel de sus rodillas.

3. Guiarás el ejercicio en voz alta. Explica a las participantes que están sentadas que van a tener un "tacto amoroso" con su compañera, la que está tumbada a su lado. La tocará y acariciará de una manera respetuosa como vas a describir a continuación. Las que no se sientan cómodas con eso pueden colocar su mano sobre la cabeza o hombro de su compañera o simplemente cerrar sus ojos y hablarles en voz baja.

4. En un tono relajado y suave, ve indicando las pautas (una cada 2-3 minutos) del ejercicio. Subraya la importancia de tomar consciencia sobre la respiración: una respiración lenta, inhalando por la nariz y exhalando por la boca.

> ***Primera indicación****: acaricia la cabeza de tu compañera.*
> ***Segunda indicación:*** *acaricia su frente.*
> ***Tercera indicación****: acaricia sus brazos.*
> ***Cuarta indicación****: acaricia sus manos y dedos.*

5. Conforme va avanzando el ejercicio, habla sobre:

> *En tanto activistas y defensoras, generalmente tenemos poco tiempo para nosotras. En este momento que estamos acariciando nuestras compañeras, estamos viviendo una oportunidad excepcional para relajarnos y sentirnos cuidadas.*

Las cargas y responsabilidades sociales que lidiamos como mujeres, defensoras, madres, hermanas. Siempre se espera de nosotras que cuidemos a los demás. ¿Y nosotras? ¿Nos cuidamos a nosotras mismas? Solemos tener muy poco espacio en nuestras vidas para el auto-cuidado o cuidado colectivo.

6. Al final de las indicaciones, dale un tiempo a las mujeres que están tumbadas de abrir los ojos e intercambiar el sitio con su compañera. Repiten el proceso con los roles intercambiados para que todas tengan la oportunidad de dar y recibir.

Referencias:

- http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos/autocuidado

Echa un vistazo

Este ejercicio es una adaptación de una parte del manual "Autocuidado y sanación feminista para ingobernables" de Mujeres Al Borde

Objetivo(s): contrarrestar sensaciones de monotonía, desencanto, tristeza y desconexión con el deseo de soñar y reconectar con la vida.

Módulo: Auto-cuidado

Duración: 20 minutos (según el tamaño del grupo)

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Sesiones y ejercicios relacionados:

- Tacto con amor (Auto-cuidado)
- Construyendo un auto-cuidado feminista (Auto-cuidado)

Materiales requeridos:

- Una mente abierta y relajada

Recomendaciones:

- El auto-cuidado es una parte esencial de la práctica de seguridad digital holística y es importante reforzarla y alentarla de manera consistente. Recomendamos distribuir los ejercicios de este módulo a lo largo de toda la capacitación.

- Para ésta y las demás sesiones de tu capacitación, procura tomar consciencia y ser sensible a las diferentes capacidades y limitaciones físicas de las participantes.

Conducir la sesión:

1. Arranca explicando como, en el día a día de activistas y defensoras, puede ser fácil abrumarse por sensaciones de monotonía, desencanto, tristeza y desconexión.

2. Durante este ejercicio, las participantes abordarán estas sensaciones que viven en el cotidiano de su lucha, donde a veces se sienten perdidas y sin norte. Activarán un punto energético que, en la medicina tradicional oriental, activa el deseo de soñar y sentirse encantada por la vida de nuevo.

3. Invita a las participantes a sentarse en círculo, ya sea en sillas o en el suelo.

4. Guía el grupo por los siguientes pasos (pídeles repetir los pasos 3 veces):

> *Localiza tu punto energético en el entrecejo, justo debajo de tus cejas y encima del puente de tu nariz.*
>
> *Inhala y mantén el aire adentro.*
>
> *Con tu pulgar, presiona tu punto energético. Conforme exhalas, piensa en algo que te inspira y te hace sentir viva.*

5. Cierra la sesión invitando a las participantes a usar esta técnica cuando se sientan con la necesidad de centrarse. Hablen sobre lo natural que es sentirse a veces con miedo, cansancio o desencanto. Todo el mundo se siente así de vez en cuando.

Referencias:

- http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos/autocuidado

Nuestras reflexiones

Objetivo(s): pensar sobre nuestras prácticas de auto-cuidado, específicamente las que llevamos a cabo y nos hacen bien, las que podemos mejorar y las que queremos adoptar.

Módulo: Auto-cuidado

Duración: 20-30 minutos (depende de ti)

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Sesiones y ejercicios relacionados:

- Yo decido (Buscando la mejor solución)
- Tacto con amor (Auto-cuidado)
- Construyendo un auto-cuidado feminista (Auto-cuidado)
- Echa un vistazo (Auto-cuidado)

Materiales requeridos:

- Un espejo por participante
- Stickers circulares pequeños
- Opcional: las participantes pueden utilizar fotos de si mismas en vez de espejos (en este caso, avísalas antes de la sesión)

Recomendaciones:

- El auto-cuidado es una parte esencial de la práctica de seguridad digital holística y es importante reforzarla y alentarla de manera consistente. Recomendamos distribuir los ejercicios de este módulo a lo largo de toda la capacitación.

- Con el fin de crear un entorno que induce a la relajación e introspección, puedes alumbrar unas velas, quemar incienso y/o poner música tranquilizante de fondo durante el ejercicio.

Conducir la sesión:

1. Entrega a cada participante un espejo pequeño o una foto de ella misma. Reparte los stickers.

2. Explica que vas a leer una serie de enunciados ante las cuales las participantes contestarán, para ellas mismas, "sí" o "no". Cada vez que contesten "no", colocarán un sticker en el espejo o foto.

3. A continuación damos ejemplos de enunciados. Puedes agregar o saltar algunas basándote en tu conocimiento previo sobre el grupo (sobre sus contextos, qué tan cómodas las percibes):

- *Duermo al menos 8 horas por día y me siento descansada cuando arranco el día.*
- *En el último año/6 meses, he tenido la oportunidad de tomarme unas vacaciones y las he aprovechado.*
- *Como de manera sana y hago ejercicio con frecuencia para mantener mi mente y cuerpo en equilibrio.*
- *Siempre encuentro un poco de tiempo para mí para leer, dormir, pasar tiempo con mis amigas y familia.*
- *Cuando enfermo, tomo unos días de descanso para recuperarme y concentrarme en estar mejor.*
- *Cuando estoy saturada, digo no a ofertas extra de trabajo.*
- *Me hago revisiones ginecológicas cada seis meses.*
- *Dedico tiempo a aclarar y resolver malos entendidos con mis seres queridos y compañera/os de trabajo cuando brotan conflictos.*
- *Mantengo una jornada de 8 horas por día de trabajo que tanto yo como mi organización respeta.*

4. Pregunta a las participantes qué ven en el espejo/foto. El grupo se junta en círculo para discutir sobre los efectos que tiene la carga excesiva de trabajo, dinámicas sociales nocivas en nuestro trabajo, la falta de cuidado sobre nuestro cuerpo y mente...

5. Invita a las que quieran a compartir una intención dirigida a cuidarnos mejor, en el sentido que se viene trabajando en la sesión.

Referencia

- http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos/autocuidado

El acto del NO

Objetivo(s): reflexionar sobre las cargas que se nos asignan como mujeres, defensoras, activistas y cómo justificar, para nosotras mismas, la necesidad del auto-cuidado.

Módulo: Auto-cuidado

Duración: 10-15 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Sesiones y ejercicios relacionados:

- Ninguno

Materiales requeridos:

- Sinceridad y sensibilidad

Recomendaciones:

- El auto-cuidado es una parte esencial de la práctica de seguridad digital holística y es importante reforzarla y alentarla de manera consistente. Recomendamos distribuir los ejercicios de este módulo a lo largo de toda la capacitación.

- Algunas pueden sentirse incómodas contando sus historias (véase a continuación). En estos casos, pueden compartir la historia de una amiga, su hermana o una compañera de trabajo.

Conducir la sesión:

1. Arranca el ejercicio hablando sobre las diferentes presiones que la sociedad ejerce sobre las mujeres. Las normas socioculturales dictaminan que las mujeres tienen que trabajar 2 o 3 veces más que los hombres para demostrar su valor, por ejemplo.

2. Continúa presentando cómo las defensoras enfrentan incluso más cargas laborales, la sensación de culpa por fallar con fechas de entrega o metas, la expectativa sobre ellas de cuidar de los demás antes que a ellas mismas.

3. En este ejercicio, tendrán la oportunidad de reflexionar sobre estas cargas con las que tienen que lidiar. El grupo se divide en parejas.

4. En cada pareja, intercambian historias sobre momentos en los que querían decir que "NO" pero no lo hicieron o no podían hacerlo. "NO" ante tener que asumir trabajo extra o cuando te pidieron un favor o cuando tenías que cumplir con otro compromiso, etc. Puedes arrancar tú contando una historia, por ejemplo:

Tenía planeado una cena con unas amigas pero en el trabajo me pidieron quedarme hasta tarde resolviendo un problema que surgió en un proyecto importante. No podía decir que "NO" aunque tenía muchas ganas de hacerlo.

5. Ahora, en parejas, volverán a contar las historias, pero esta vez van a narrarlas como si hubieran dicho "NO".

6. Pueden incluir en esas historias cómo explicaron a los demás por qué están diciendo que "NO". Aunque no sea necesario como tal, puede ser una reflexión saludable sobre la importancia de hacer tiempo para nosotras mismas.

Una carta de amor a mí misma

Objetivo(s): brindar espacio y tiempo a las defensoras para que puedan pensar sobre sí mismas, además de compartir sus preocupaciones y acciones que pueden tomar para aliviar las presiones que enfrentan.

Módulo: Auto-cuidado

Duración: 20 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Sesiones y ejercicios relacionados:
- Ninguno

Materiales requeridos:
- Material de papelería
- Proyector y computadora
- Opcional: si prefieres no usar un proyector, puedes escribir las frases en un papel grande o pizarrón.

Recomendaciones:
- El auto-cuidado es una parte esencial de la práctica de seguridad digital holística y es importante reforzarla y alentarla de manera consistente. Recomendamos distribuir los ejercicios de este módulo a lo largo de toda la capacitación.

- Según el grupo con el que estés trabajando y el tiempo disponible, considera cerrar esta actividad reflexionando sobre qué es el auto-cuidado y su relevancia. Pregúntale a las participantes: ¿Cuándo fue la última vez que se preguntaron cómo se sentían? ¿Creen que su activismo impacta su salud? ¿Cómo están cuidándose a ellas mismas, el recurso más importante en su activismo?

Conducir la sesión:

1. Proyecta una diapositiva o muestra un papel grande que tenga escrito lo siguiente:

    Querida _____,

    Te he estado observando últimamente y sé que estás teniendo dificultades con...

    También sé que te preocupa...

    Sólo quería que supieras que...

    Recuerda que eres muy buena en/haciendo...

    Creo que podrías...

    E intenta hacer... las siguientes semanas.

    Con amor,
    tú misma

2. Entrega un papel a cada participante y pídeles rellenar los espacios en blanco.

3. No tendrán que compartir la carta con las demás. Se trata de una actividad muy personal.

Ejercicios de cierre y evaluación

Vamos dando cierre a nuestro taller. Repasar lo que aprendimos juntas y conducir nuestro proceso de taller hacia conclusiones constructivas.

Aquelarre de brujas

Objetivo(s): agilizar las energías y estimular el grupo. Un paréntesis menos "técnico" sobre seguridad digital.

Módulo: Ejercicios de cierre y evaluación

Duración: 10 a 15 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Sesiones y ejercicios relacionados:

- Her-Story (las historias de las mujeres) de las tecnologías (Repensando nuestra relación con las tecnologías)

Material requerido:

- Sillas (una menos que el número de participantes)

Conducir la sesión:

1. Pregunta al grupo si están familiarizadas con el juego de las sillas musicales. Ahora explica el juego en clave feminista.

2. Colocan las sillas en círculo. Todas buscan un asiento. Una compañera se queda sin uno.

3. Asigna a cada participante el nombre de una mujer destacada en la historia de las tecnologías o feminismos. Puedes utilizar los mismos nombres de la sesión "Her-story (la historia de las mujeres) en las tecnologías". Asigna cada nombre a varias participantes.

4. Explica qué es un "aquelarre de brujas": un encuentro nocturno entre brujas donde se cuentan historias y hacen conjuros. En esta sesión van a crear su propio aquelarre.

5. Arranca el aquelarre inventando una historia sobre las mujeres que están homenajeando:

- Cada vez que mencionas el nombre de estas mujeres, las participantes que tienen ese nombre asignado intercambiarán asientos.

- La persona que se queda sin asiento (puede sentarse en el suelo y) continúa la historia y menciona otro nombre.

- Si en la historia sale la palabra "aquelarre", todas intercambian asiento.

6. Repite varias veces hasta que todos los nombres se hayan dicho en voz alta o hasta que todas hayan podido participar en la creación de la historia.

La Caldera

Objetivo(s): equilibrar el nivel de participación del grupo. Dentro de un grupo, algunas personas hablan más que otras. Este ejercicio sirve para generar conciencia de este hecho e invitar a participantes que no han hablado tanto a hacerlo.

Módulo: Ejercicios de cierre y evaluación

Duración: 15-20 minutos (según el tamaño del grupo)

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Sesiones y ejercicios relacionados:
- Ninguno

Materiales requeridos:
- Tiras de papeles (3-5 por participante)
- Recipiente/cuenco/cesta

Recomendaciones:
- La caldera puede ser un elemento útil en el taller. Si realizan esta sesión al comienzo, pueden utilizar este ejercicio cada vez que haces una pregunta al grupo. De esta manera, cada quien tiene más oportunidad de participar, incluyendo las personas más tímidas.

- Este ejercicio girará en torno a una discusión grupal que puede ser sobre lo que quieran; sin embargo, funciona mejor si se centran en un tema relacionado con el taller. Puedes introducir un tema nuevo o puedes repasar un tema ya discutido anteriormente.

Conducir la sesión:

1. Todas se sienten en círculo alrededor de un recipiente que representará una "caldera". Entrega a cada persona entre 3 y 5 tiras de papel.

2. Cada vez que alguien habla, tirarán uno de sus papeles dentro de la caldera. Si alguien se queda sin papeles, deja de hablar.

3. Introduce un tema y facilita la discusión haciendo preguntas. Por ejemplo, si fuera sobre malware y virus, podrías preguntar:

- ¿Qué es malware?
- ¿Cuáles son los tipos que conoces?
- ¿Hay sistemas operativos que son inmunes a infección de malware?
- ¿Alguna vez se ha infectado tu computadora o celular de malware? ¿Cómo se dieron cuenta?
- ¿De qué maneras podemos proteger nuestros dispositivos ante infecciones de malware?

4. Continúa la discusión hasta que todo el mundo se quede sin tiras de papel. Puedes hacer una segunda vuelta de discusión cambiando de tema y devolviendo los papeles a cada participante.

Flores feministas

Objetivo(s): tras un día intenso de talleres de seguridad digital (especialmente los primeros días), vamos a despertar una dosis de motivación e inspiración.

Módulo: Ejercicios de cierre y evaluación

Duración: 10 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Sesiones y ejercicios relacionados:
- Ninguno

Materiales requeridos:
- Tiras de papeles
- Lapicero, bolígrafo, pluma
- Flores (reales o de plástico/papel)

Recomendaciones:
- Este ejercicio se puede repetir a lo largo de la capacitación.
- Si no puedes conseguir flores naturales, puedes seguir este video: https://www.youtube.com/watch?v=EuNYKO9WfAE

Conducir la sesión:

1. Antes de arrancar el ejercicio, necesitarás preparar algunas cosas:

- Escribe mensajes cortos y alentadores en tiras de papel. Aquí van algunos ejemplos:

  Después de esta experiencia, no voy a necesitar de una "persona técnica".
  Hay una comunidad de mujeres/feministas que me respaldan.

Respiro hondo y hago reset.
Puedo hacer ésto. He hecho cosas más difíciles en el pasado.
Mis dispositivos no tienen poderes mágicos sobre mí. Yo tengo el control.
Yo soy la única persona que puede decidir sobre cómo practico la seguridad digital.

- Coloca un papel en cada flor.

2. El grupo se siente en círculo y responde a la siguiente pregunta: "¿Con qué frecuencia te sientes frustrada o abrumada con las tecnologías? Recuerda al grupo que es totalmente normal sentirse así.

3. Entrega una flor a cada participante. No abrirán los papeles aún.

4. Cuenta una experiencia donde te sentiste frustrada desde tu rol de facilitadora o cuando estabas empezando en el ámbito de la seguridad digital. Cada quién puede remitirse a sus propias experiencias de desafíos con las tecnologías. No hay nada que no puedan superar juntas.

5. Abren sus flores y, una por una, leen en voz alta los mensajes. Invítalas a compartir cómo se han sentido en la sesión, que conclusiones han sacado, qué significa el mensaje dentro de la flor para ellas.

Círculo mágico

Objetivo(s): cerrar proyectando intenciones para seguir compartiendo con las demás lo que han aprendido.

Módulo: Ejercicios de cierre y evaluación

Duración: 30 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Ninguno requerido

Sesiones y ejercicios relacionados:

- Ninguno

Materiales requeridos:

- Papel y lapicero

Conducir la sesión:

1. Las experiencias y conocimientos nuevos son más ricos si se comparten y complementan con las demás. Explica que la intención de este ejercicio es hacer un cierre proyectando intenciones para seguir compartiendo con las demás lo que han aprendido.

2. Forman un círculo sentadas (en sillas o en el suelo) o de pie. Lo que sea más cómodo para todas.

3. Ofrece un contexto al ejercicio explicando sobre el simbolismo del círculo.

- Desde la prehistoria, la disposición circular es esencial en la celebración de rituales. Se creía que la energía que se genera entre personas dentro de un círculo exorciza los espíritus malos y atrae los espíritus buenos.

- Dentro de un círculo, las personas se ven todas desde una misma distancia. Cada persona ocupa el mismo lugar y plano. El liderazgo se confía, no se disputa.

- Los círculos equilibran los flujos de energía: cada persona recibe y entrega, nadie antecede a otra.

4. Cada participante escribe en un papel algo que está dispuesta a compartir con la persona a su derecha. Puede ser cualquier cosa: un pensamiento, una canción, un poema, algo que aprendieron en el taller.

5. Doblan el papel y lo sostienen en su mano derecha. La mano derecha simboliza nuestra habilidad de ayudar a las demás. La mano izquierda representa la necesidad de intercambiar. Juntan sus manos en círculo.

6. Colocan su papel, con la mano derecha, en la mano izquierda de la compañera.

7. Lee el papel que recibiste. Puede ser en voz alta o sólo para ti.

8. Mientras vas leyendo los papeles, explica la idea de sororidad: el amor entre mujeres que se perciben como pares y aliadas; construir solidaridad a partir de la violencia, desigualdad e injusticias que enfrentamos; transformar positivamente nuestras realidades. Juntas nos apoyamos en sororidad, compartiendo conocimientos y reflexiones.

¡Adivinanzas!

Objetivo(s): las capacitaciones suelen ser bastante intensivas con mucha información a absorber en poco tiempo. Este ejercicio es una herramienta que puedes utilizar para evaluar el conocimiento y entendimiento de las participantes dentro de un contexto lúdico y relajante.

Módulo: Ejercicios de cierre y evaluación

Duración: 15 minutos

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:
- Ninguno requerido

Sesiones y ejercicios relacionados:
- Ninguno

Materiales requeridos:
- Fichas de seguridad digital
- Cinta o pinzas para la ropa
- Música (para poner de fondo)

Recomendaciones:
- Las que vayan completando el ejercicio pueden ayudar a sus compañeras .

Conducir la sesión:
1. Todas se colocan en fila, dando la espalda a la facilitadora. Coloca con una pinza o cinta una ficha en la espalda de cada participante. Asegúrate que nadie vea la ficha que les tocó.

2. Las participantes se distribuyen por el espacio. Cada ficha representa un concepto o herramienta que han discutido en el taller.

3. Pon música e indica a las chicas moverse por la sala. Se pueden estirar, bailar, andar o moverse como quieran. Cuando paras la música, las chicas se paran también.

4. Buscan a la compañera que les queda más cerca. Se muestran, las unas a las otras, la ficha que tienen en su espalda y la otra compañera intentará explicar cuál es la ficha de la otra a través de lenguaje no verbal. Cuando la compañera haya adivinado su ficha, rotan papeles. El ejercicio finaliza cuando todas hayan adivinado su ficha.

Yincana DigiSec

Objetivo(s): con el fin de dar cierre al taller con energía, realizarán una yincana para repasar todo lo que han aprendido.

Módulo: Ejercicios de cierre y evaluación

Duración: 45 minutos (según las participantes)

Formato: Ejercicio

Nivel de habilidades: Básico

Conocimientos requeridos:

- Variable según los contenidos que se han cubierto en la capacitación.

Sesiones y ejercicios relacionados:

- Variable según los contenidos que se han cubierto en la capacitación.

Materiales requeridos:

- Espacio grande al aire libre o espacio interior con diferentes salas y pasillos.
- Fichas con preguntas (una para cada participante)
- Marcadores, lapiceros y papel.

Recomendaciones:

- Los estudios de caso que van a utilizar en el rally depende de lo que hayan visto en el taller. Se recomienda realizar esta sesión al final porque repasa todo lo que aprendieron juntas. También permite identificar qué cosas comprendieron mejor y cuáles podrían requerir de más apoyo.

- La idea es brindar una oportunidad práctica y dinámica para aplicar todo lo repasado en las sesiones previas. Por ello, los casos están enfocados a respuestas directas a incidentes más que medidas de prevención.

Conducir la sesión:

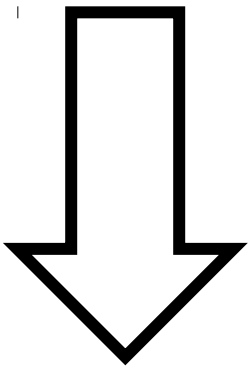
Parte 1 – Planeando la ruta de la yincana

1. Antes de comenzar, decide cuántas estaciones y casos va a tener el rally. En este ejemplo que compartimos hay 5. No te olvides de incluir instrucciones en cada caso de a qué estación ir después de resolver el caso.

2. Distribuye las cinco estaciones en el espacio. Puede ser en una misma sala o en varias salas sí tienen acceso. Este ejercicio funciona mejor si cuentan con diferentes ambientes porque crea un clima más dinámico. Si puedes, intenta hacer el rally en un lugar diferente al espacio donde estuvieron durante todo el taller para dar un aire de cambio.

3. En cada estación, las participantes tendrán que resolver un caso con todo lo que aprendieron hasta ahora, con ayuda del kit de herramientas que compartimos a continuación. Recomendamos que se dividan en grupos para dinamizar el rally y no saturar cada estación.

Aquí van algunos materiales que necesitarás para el rally.



Material 1: Orden de estaciones y ruta

EQUIPO 1	**EQUIPO 2**
Estación 1 (Inicio)	***Estación 5 (Inicio)***
Estación 2	Estación 3
Estación 3	Estación 1
Estación 4	Estación 2
Estación 5	Estación 4
META FINAL	

Material 2: Caja de herramientas

Número.	Herramienta
1	Red Privada Virtual/ Virtual Private Network (VPN)
2	Programa de Antivirus
3	Navegador Tor & Cuenta de correo anónimo
4	Cifrado (llaves GPG)
5	Protocolo de seguridad
6	Medidas de respuesta inmediata
7	Modelo de riesgos con perspectiva de género

Material 3: Ejemplos de casos

CASO #1

Una directora de cine acaba de terminar su documental sobre desaparición forzada en México. Se va ya de tarde-noche de la oficina, después de una reunión, con la intención de llegar a casa y enviar el documental a sus colaboradora/es y familiares, también a las víctimas y especialistas entrevistadas en el proyecto. Pero, al llegar, descubre que han saqueado su casa y, lo que es peor aún, que desapareció su computadora donde tenía el documental (y no tiene respaldo). ¿Qué aconsejas en esta situación?

Ejemplo de respuesta

Herramienta a utilizar (del kit de herramientas):
Medidas de respuesta inmediata

Recomendaciones:

- Notificar a sus contactos de lo ocurrido, especialmente a las personas involucradas en el documental.

- Cambiar todas las contraseñas de sus cuentas online y habilitar autenticación de dos factores en todas las cuentas posibles.

- Establecer un protocolo de seguridad para manejar y distribuir materiales de grabación en el futuro.

- Preguntarle si tiene respaldos físicos o subidos a internet de material de grabación sin editar, entrevistas, imágenes, etc. que pueda recuperar y almacenar de manera segura.

- Revisar todos los archivos que pueda recuperar, localizar dispositivos y equipo que utilizó para grabar y editar el documental.

CASO #2

Olga es una activista. Va a empezar a trabajar con un grupo de mujeres activistas para documentar casos de feminicidio en México. Van a necesitar compartir documentos en línea y discutir información confidencial por teléfono. Algunas de estas mujeres tendrán que desplazarse a determinadas ciudades para hacer entrevistas a familias. ¿Qué recomiendas?

Ejemplo de respuesta

Herramienta a utilizar (del kit de herramientas):
Protocolos de seguridad.

Recomendaciones:
Realizar una reunión grupal para realizar un análisis de riesgos.

Acordar una serie de medidas de seguridad digital, incluyendo protocolos específicos para viajes, que el grupo tendrá que implementar.

Acordar utilizar una app segura para intercambiar mensajes como Signal.

Explorar maneras seguras de intercambiar documentos: cifrarlos con GPG o enviarlos a través de una cuenta más segura de correo como Tutanota o Riseup.

CASO #3

Nelly es la coordinadora de un proyecto abocado a la justicia para mujeres en su país. La invitaron a dar una presentación en otro país. En el aeropuerto se da cuenta que ya no tiene datos en su plan celular y decide no renovarlo ya que se va de viaje. Mientras espera su avión, quiere conectarse al WiFi del aeropuerto y echar un vistazo a su correo. ¿Qué debería hacer?

Ejemplo de respuesta

Herramienta a utilizar (del kit de herramientas):
VPN

CASO #4

Ariadna es una periodista ecuatoriana que trabaja en una investigación sobre desviación de fondos. Manda solicitudes de información a entidades gubernamentales en su país. ¿Qué le aconsejas que haga para realizar esta documentación de manera segura?

Respuesta de ejemplo

Herramienta a utilizar (del kit de herramientas):
Navegador Tor y cuenta de correo anónima.

CASO #5

Una colectiva feminista que defiende el derecho a decidir de las mujeres está siendo acosada desde hace una semana en plataformas de redes sociales. ¿Qué pueden hacer para protegerse?

Respuesta de ejemplo

Herramienta a utilizar (del kit de herramientas):
Modelo de riesgos con perspectiva de género

Recomendaciones:
El colectivo puede analizar los potenciales riesgos ante estos ataques, el impacto que pueden tener y la probabilidad de que el riesgo aumente o escale la violencia, además de definir las herramientas y estrategias que pueden implementar.

Parte 2 - 1,2, 3... ¡lista!

4. Divide las participantes en grupos según cuántas sean (máximo 5 por grupo para procurar una buena participación colectiva). Cada grupo escogerá una manera creativa y lúdica de nombrarse.

5. Explica las reglas de la Yincana DigiSec:

- Según las rutas y el orden de las estaciones definidas en la guía correspondiente, indica a cada grupo dónde empezar y en cuál van a acabar la yincana. Asegúrate de señalar todas las paradas a las participantes antes de comenzar para que no se pierdan.
- En cada parada, el grupo resolverá un caso, aplicando todo lo que han aprendido hasta ahora y ayudándose del kit de casos que recibieron. Pueden ser creativas a la hora de responder: como en todo, ninguna solución funciona para todas.
- Dé un tiempo para que los grupos se preparen. Una vez que estén listas, haz la cuenta regresiva para arrancar.
- El primer grupo en resolver todos los casos y volver a la estación final que les corresponde, gana.

6. Una vez que hayan terminado, se colocarán en círculo. Cada equipo explica sus respuestas a cada caso y cómo llegaron a ellas. Retroalimenta las explicaciones de los grupos.

APÉNDICES

Herramienta de seguridad digital y capacidades (DISC)
Documento interno con puntuaciones

Se puede aplicar al comienzo de la capacitación como punto de referencia y después volver a realizar cada 6 meses. También se puede utilizar a modo de evaluación al final del taller.

A continuación encontrarás una serie de preguntas que permitirán a las personas facilitadoras comprender el nivel que tienen las personas dentro de la organización en cuanto a prácticas de seguridad digital. Además, permite monitorear los avances de las participantes en las capacitaciones. Los resultados sirven meramente como evaluación y se compartirán de manera anónima con IWPR y las demás entidades donantes de este proyecto.

País _____

En tu organización:

1. ¿Con qué frecuencia actualizan los sistemas operativos y software que utilizan? (rodea la opción):

- Nunca (0 puntos)
- En los últimos 6 meses (1 punto)
- En los últimos 30 días (4 puntos)
- En los últimos 15 días (5 puntos)
- Hace más de 6 meses (0 puntos)
- Tenemos el sistema operativo más nuevo en esta computadora (5 puntos)
- Las estamos actualizando ahora (3 puntos)
- No sé (0 puntos)

2. ¿Con qué frecuencia respaldan sus datos en un disco duro externo o en un servicio de archivos en "la nube"? (rodea la opción):

- Nunca (0 puntos)
- Hace más de un año (0 puntos)
- En el último año (1 punto)
- En los últimos 6 meses (2 puntos)
- En los últimos 60 días (3 puntos)
- En los últimos 30 días (4 puntos)
- Respaldamos los datos en las últimas dos semanas (5 puntos)
- No sé (0 puntos)

3. Cifrado de disco duro externo o de archivos alojados "en la nube"

- Sí, ambos están cifrados (5 puntos)

- No (0 puntos)
- Sólo un de ellos está cifrado (3 puntos)
- No sé (0 puntos)

Si respondiste que sí, ¿qué herramienta de cifrado utilizas? _____

4. El software instalado en mi computadora de trabajo ¿es original y tiene licencia? (por ej., Microsoft Windows, Microsoft Office, Adobe Photoshop, Adobe Illustrator, Corel Draw, Antivirus), ¿es software open source? (Open Office, Scribus).

- Todos los programas están pirateados (0 puntos)
- Algunos de los programas están pirateados (1 punto)
- La mayoría de los programados son originales y tienen licencia (2 puntos)
- Todos los programas son originales y tienen licencia (5 puntos)
- La mayoría de los programas son open source (2 puntos)
- Todos los programas son open source (5 puntos)
- No estoy segura (0 puntos)

5. Uso programas anti-virus en mi computadora y celular de trabajo, están actualizados y los inicio cada vez que enciendo mis dispositivos.

- Sí, en mi computadora y en mi celular (5 puntos)
- Sólo en mi computadora (3 puntos)
- Sólo en mi celular (3 puntos)
- No tengo anti-virus (0 puntos)
- No sé (0 puntos)

En caso afirmativo, ¿qué anti-virus usas en tu computadora?_____
En caso afirmativo, ¿qué anti-virus usas en tu celular? _____

6. Bloqueo la pantalla de mi computadora y celular de trabajo con una contraseña.

- Sí (5 puntos)
- No (0 puntos)
- Sólo uno de ellos tiene contraseña (2 puntos)

7. La red Wi-Fi que utilizo para trabajar tiene una contraseña diferente a la que entregó el proveedor de servicio de internet. Además, cumple con los criterios de una contraseña robusta: incluye al menos 25 caracteres, letras y números, caracteres especiales, minúsculas y mayúsculas.

- Sí - la contraseña está cambiada y cumple al menos dos de los criterios anteriores (5 puntos)
- No - es la misma contraseña que nos dieron al contratar el servicio (0 puntos)
- Parcialmente - cumple uno de los criterios de los anteriores (3 puntos)
- Parcialmente - la contraseña está cambiada pero no cumple ninguno de los criterios (1 punto)

8. ¿Utilizas WiFi público en hoteles, aeropuertos, cafés, etc?

- Nunca uso redes públicas de Wi-Fi en hoteles, aeropuertos o café al menos que esté conectada a un servicio de VPN (5 puntos)
- A veces uso redes públicas de Wi-Fi en hoteles, aeropuertos o cafés sin conectarme a un servicio de VPN (2 puntos)
- Siempre uso redes públicas de Wi-Fi en hoteles, aeropuertos o cafés sin servicio VPN (0 puntos)

9. ¿Utilizas herramientas de cifrado para guardar documentos en tu computadora?

- Sí (5 puntos)
- No (0 puntos)
- Sólo para algunos documentos (3 puntos)

Si contestaste que sí, ¿qué herramienta utilizas? _____

10. ¿Utilizas herramientas de cifrado para enviar texto a través de correo electrónico o SMS entre las personsa integrantes de tu organización?

- Siempre uso cifrado para mi correo, SMS o chats para transmitir datos confidenciales (5 puntos)
- Suelo usar cifrado para mi correo, SMS o chats para transmitir datos confidenciales (3 puntos)
- Casi nunca uso cifrado para mi correo, SMS o chats para transmitir datos confidenciales (2 puntos)
- Nunca uso cifrado para mi correo, SMS o chats para transmitir datos confidenciales (0 puntos)

11. ¿Con quién compartes tus contraseñas?:

- Compañera/o íntima/o (0 puntos)
- Familiares (0 puntos)
- Mejor amiga/o (0 puntos)
- Compañera/os de trabajo (0 puntos)
- Nadie (5 puntos)

12. ¿Utilizas contraseñas robustas con al menos 25 caracteres, letras, números, caracteres especiales, minúsculas y mayúsculas; sin palabras de diccionario, fechas de cumpleaños o información personal? ¿Todas tus contraseñas cumplen con los criterios anteriores?

- Sí (5 puntos)
- No (0 puntos)
- Sólo algunas (3 puntos)

13. ¿Tienes diferentes contraseñas para cada dispositivo y cuenta (computadora, teléfono, correo electrónico, cuentas de plataformas de redes sociales, banco, etc.)?

- Sí (5 puntos)
- No (0 puntos)
- Tengo diferentes contraseñas, pero a veces repito algunas (1 punto)
- Algunas contraseñas están establecidas por defecto por mi organización/oficina/proveedor de servicio (3 puntos)

14. ¿Has tomado una decisión estratégica sobre cómo manejar tus identididades en plataformas de redes sociales, tanto a nivel personal como en tu activismo, basándote en tu nivel de riesgos?
(Por ejemplo, usar diferentes identidades y cuentas o usar identidades/cuentas falsas para el activismo y para el trabajo; compartir abiertamente utilizando tu nombre, foto e identidad real si no te sientes bajo amenaza).

- Sí - Lo he considerado y me siento segura con el manejo actual que tengo de mis identidades online (5 puntos)
- No - No he pensado sobre ello (0 puntos)
- Parcialmente - Creo que tiene sentido crear diferentes cuentas o cuentas anónimas, pero no he hecho cambios todavía (2 puntos)
- Parcialmente - He considerado el manejo de mis identidades online y he realizado cambios, pero no tengo certeza si la configuración es segura (4 puntos)
- En mi situación, me hace más sentido usar mi propio nombre e identidad real en todas mis cuentas de plataformas de redes sociales (5 puntos)

15. ¿Almacenas tus contraseñas en un gestor de llaves seguro protegido con contraseña maestra?

- Sí (5 puntos)
- No (0 puntos)
- Sólo algunas cuentas (3 puntos)
- ¿Qué es eso? (0 puntos)

En caso afirmativo, ¿dónde está almacenado el gestor de llaves y en qué formato?

_____

15. Cuando navegas, ¿siempre lo haces vía HTTPS?

- Sí (5 puntos)
- No (0 puntos)
- ¿Qué es eso? (0 puntos)
- Siempre verifico, pero no es siempre posible navegar con HTTPS (3 puntos)

16. Sobre tus cuentas en plataformas de redes sociales

- Todos mis posts son públicos (0 puntos)
- No sé quién puede ver lo que publico (0 puntos)
- Escojo configuraciones específicas para cada post (4 puntos)
- Ajusto la configuración para controlar quién puede ver qué información en mis cuentas (5 puntos)
- No sé cómo modificar las configuraciones de mis cuentas (0 puntos)

17. ¿Cuándo haces click en enlaces o abres adjuntos en correos?

- Cuando parecen contener información importante o urgente (0 puntos)
- Cuando conozco la persona que lo está enviando, pero no el mail desde donde lo está enviando (ej. parejas sentimentales, viejas amistades...) (1 punto)
- Cuando proceden de una red de confianza (2 puntos)
- Cuando estaba esperando el correo (3 puntos)
- Cuando conozco y verifico la identidad de la persona que lo envía (5 puntos)

18. ¿Usas herramientas de comunicación cifrada? (chat, llamadas de video y voz, VOIP)

- Sí (5 puntos)
- No (0 puntos)
- A veces (2 puntos)
- No sé lo que es eso (0 puntos)

¿Qué herramientas más seguras utilizas?

_____

19. ¿Usas reguladores de potencia para proteger mis dispositivos electrónicos de valor?

- Sí (5 puntos)
- No (0 puntos)
- Sólo en mi oficina (2 puntos)
- Sólo en casa (2 puntos)
- Sólo en algunos dispositivos (2 puntos)

Suma todos los puntos y regístralos en la tarjeta de puntuación. ____ puntos/ 100 puntos