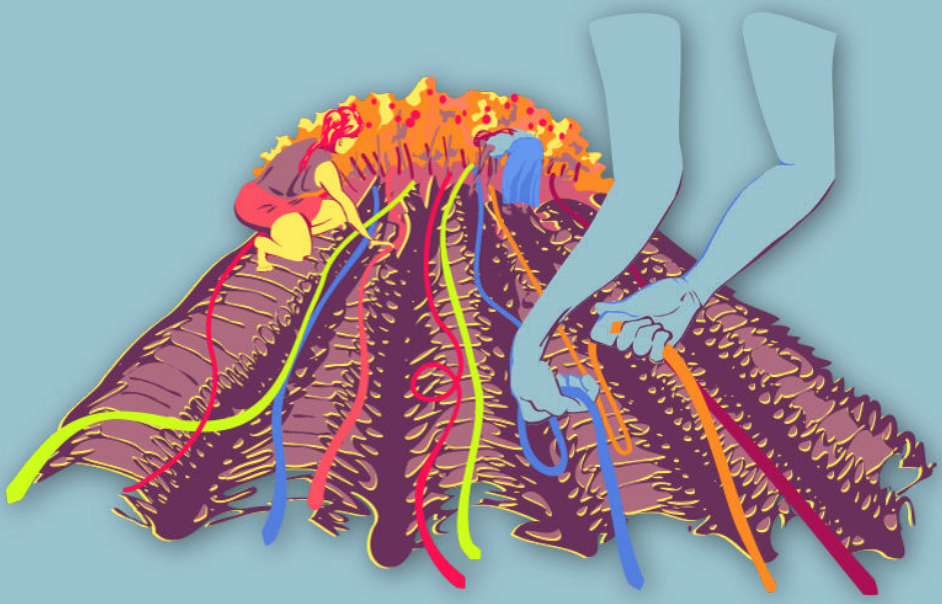
CIBERMUJERES



Buscando la mejor solución

Buscando la mejor solución

https://iwpr.net/

Índice general

Modelo de riesgos con perspectiva de género

- **Objetivos:** Identificar riesgos específicos que enfrentamos como mujeres y defensoras; diseñar estrategias de seguridad que aborden dichos riesgos.
- **Duración:** 40-50 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Varias (véase "Recomendaciones" a continuación)
- **Sesiones y ejercicios relacionados:**
  - ¡Empecemos a crear un diario de documentación![1]
  - Planes y protocolos de seguridad en organizaciones[2]
- **Materiales requeridos:**
  - Marcadores de colores
  - Rotafolio o pizarrón

[1] https://cyber-women.com/es/violencia-en-línea-contra-las-mujeres/empecemos-a-crear-un-diario-de-documentación/

[2] https://cyber-women.com/es/planeando-con-anticipación/planes-y-protocolos-de-seguridad-en-organizaciones/

- **Recomendaciones:** Esta sesión se puede facilitar de varias maneras: (a)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.; (b)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; (c) 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 probabilidad 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 siguien-

te 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.

Probabilidad (P): 1 = Muy bajo; 5 = Muy alto

Riesgo digital	P
¡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 dimensio-

nar 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.

Probabilidad (P): 1 = Muy bajo; 5 = Muy alto / **Impacto (I):** 1 = Gravedad/severidad/intensidad baja; 5 = Gravedad/severidad/intensidad alta / **Reacción (R):** 1 = Tranquilo, bajo control; 5 = Pánico, alto estrés

Riesgo digital	P	I	R
¡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 anterior-

mente 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:

Probabilidad (P): 1 = Muy bajo; 5 = Muy alto / **Impacto (I):** 1 = Gravedad/severidad/intensidad baja; 5 = Gravedad/severidad/intensidad alta / **Reacción (R):** 1 = Tranquilo, bajo control; 5 = Pánico, alto estrés

Riesgo digital	P	I	R	¿Qué puedo hacer?
[...]	4	3	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.
[...]	2	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

- **Objetivos:** 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.
- **Duración:** 90 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
- **Sesiones y ejercicios relacionados:**
  - Impresiones personales sobre la seguridad[1]
  - ¿En quién confías?[2]
  - ¿Cómo funciona Internet?[3]

[1] https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/impresiones-personales-sobre-la-seguridad/

[2] https://cyber-women.com/es/ejercicios-para-fortalecer-la-confianza/en-quién-confías/

[3] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[4]
- **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

[4] https://cyber-women.com/es/privacidad/apps-y-plataformas-online/

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)[5]
    - Security in a Box (Frontline Defenders & Tactical Technology Collective)[6]
    - Autoprotección Digital Contra La Vigilancia (Electronic Frontier Foundation)[7]
    - Genios de Internet (Español) (Karisma Foundation)[8]

    Opcional: pueden listar diferentes organizaciones que siguen (online, en Twitter, etc.) para obtener información sobre seguridad digital en contextos locales.

[5] https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es
[6] https://securityinabox.org/es
[7] https://ssd.eff.org/es/module/eligiendo-tus-herramientas
[8] https://karisma.org.co/genios-de-internet-una-guia-para-mejorar-tu-seguridad-en-la-red

Referencias

- https://www.seguridad.unam.mx

Yo decido

- **Objetivos:** 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.
- **Duración:** 15 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Práctica con herramientas y prácticas de seguridad digital
  - Toma de decisiones sobre seguridad digital[1]
- **Sesiones y ejercicios relacionados:**
  - Impresiones personales sobre la seguridad[2]
  - ¿En quién confías?[3]
  - ¿Cómo funciona Internet?[4]

[1] https://cyber-women.com/es/buscando-la-mejor-solución/toma-de-decisiones-en-torno-a-la-seguridad-digital/

[2] https://cyber-women.com/es/repensar-nuestra-relación-con-las-tecnologías/impresiones-personales-sobre-la-seguridad/

[3] https://cyber-women.com/es/ejercicios-para-fortalecer-la-confianza/en-quién-confías/

[4] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-funciona-internet/

  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[5]
  - Toma de decisiones sobre seguridad digital[6]
- **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.

[5] https://cyber-women.com/es/privacidad/apps-y-plataformas-online/

[6] https://cyber-women.com/es/buscando-la-mejor-solución/toma-de-decisiones-en-torno-a-la-seguridad-digital/

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.