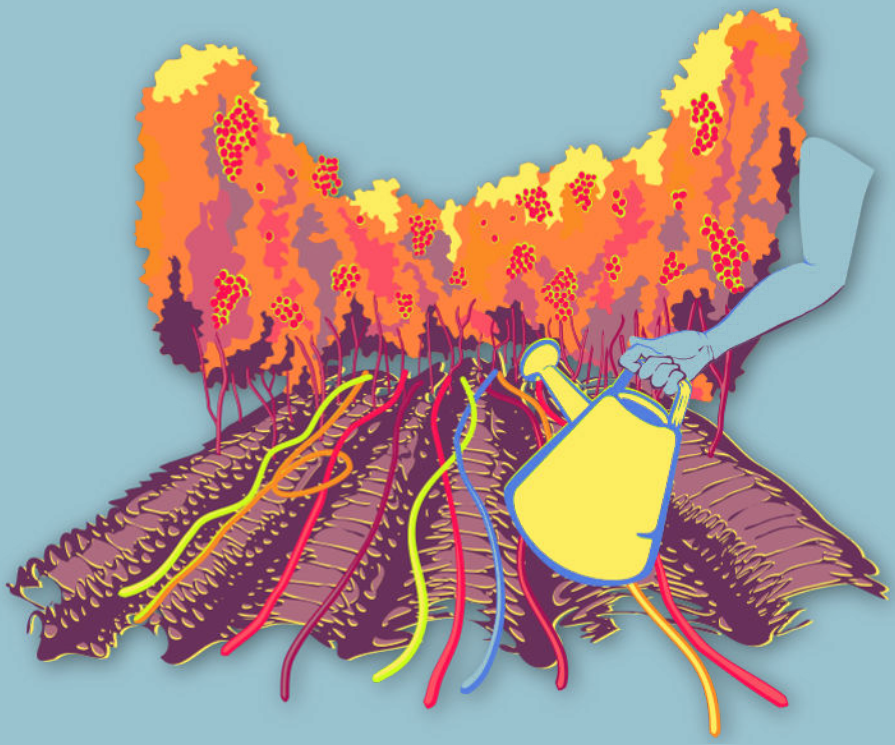
CIBERMUJERES



Planeando con anticipación

Planes y protocolos de seguridad en organizaciones

https://iwpr.net/

Índice general

Planes y protocolos de seguridad en organizaciones

- **Objetivos:** Desarrollar un plan y protocolos de seguridad para implementar medidas de seguridad digital en su propia organización.
- **Duración:** 90 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Familiaridad con herramientas y prácticas de seguridad digital
  - ¿En quién confías?[1]
  - Modelo de riesgos con perspectiva de género[2]
- **Sesiones y ejercicios relacionados:**
  - Impresiones personales sobre la seguridad[3]
  - ¿En quién confías?[4]

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

[2] https://cyber-women.com/es/buscando-la-mejor-solución/modelo-de-riesgos-con-perspectiva-de-genero/

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

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

  - ¿Cómo funciona Internet?[5]
  - Modelo de riesgos con perspectiva de género[6]
  - Planes y protocolos de seguridad digital: replicar después del taller[7]
- **Materiales requeridos:**
  - Modelo de riesgos del ejercicio
  - Modelo de riesgos con perspectiva de género[8]
- **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.

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

[6] https://cyber-women.com/es/buscando-la-mejor-solución/modelo-de-riesgos-con-perspectiva-de-genero/

[7] https://cyber-women.com/es/planeando-con-anticipación/planes-y-protocolos-de-seguridad-digital-replicar-despues-del-taller/

[8] https://cyber-women.com/es/buscando-la-mejor-solución/modelo-de-riesgos-con-perspectiva-de-genero/

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 columna).

Amenazas y riesgos	¿Qué amenazas y riesgos estamos enfrentando en la actualidad? ¿Cuáles vamos a encarar potencialmente en el futuro?
Vulnerabilidades identificadas	¿Qué prácticas individuales o circunstancias dentro de una organización pueden exponernos a algun daño?
Fortalezas y capacidades	¿Qué fortalezas tenemos como organización frente a amenazas y riesgos identificados?
Mitigar acciones	¿Qué medidas tenemos que tomar para mitigar riesgos identificados? ¿Qué podemos hacer para estar más preparadas?
Recursos requeridos	¿Qué recursos (económicos, humanos, etc.) necesitamos para implementar estas acciones?
¿Quién tiene que estar involucrada?	¿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://vrr.im/bf39