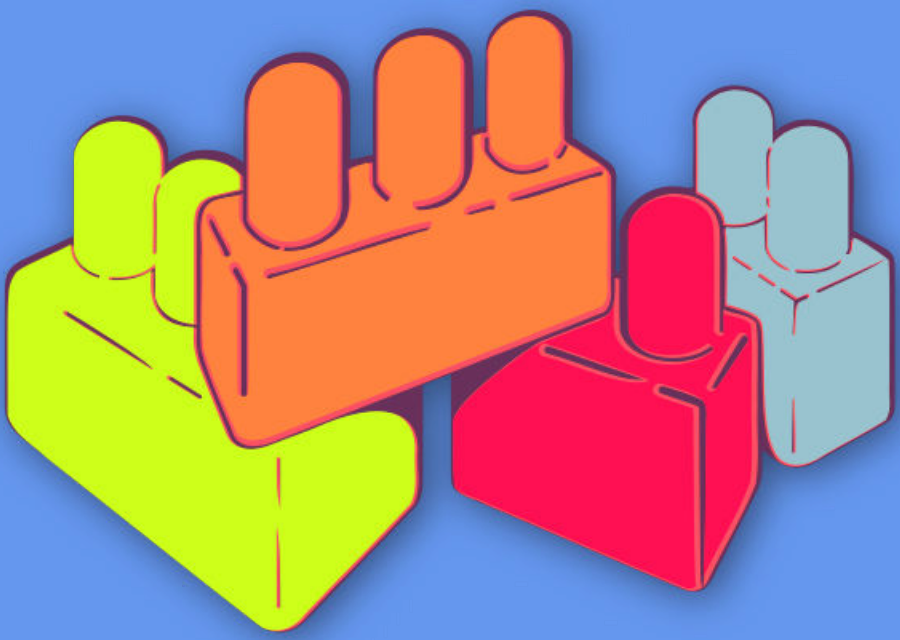
CIBERMUJERES



Principios básicos de seguridad digital 2

Almacenamiento y cifrado

https://iwpr.net/

Índice general

Almacenamiento y cifrado

- **Objetivos:** Reforzar la importancia de realizar respaldos regulares de nuestros datos y discutir cómo prevenir la manipulación y acceso sin consentimiento a nuestra información.
- **Duración:** 90 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
  - Introducción al cifrado[1]
  - Cómo hacer más segura tu computadora[2]
- **Sesiones y ejercicios relacionados:**
  - Privacidad[3]
  - Campañas online más seguras[4]
  - Introducción al cifrado[5]

[1] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

[2] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-hacer-más-segura-tu-computadora/

[3] https://cyber-women.com/es/privacidad/privacidad/

[4] https://cyber-women.com/es/activismo-online-más-seguro/campañas-online-más-seguras/

[5] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

  - Cómo hacer más segura tu computadora[6]
- **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

[6] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/cómo-hacer-más-segura-tu-computadora/

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