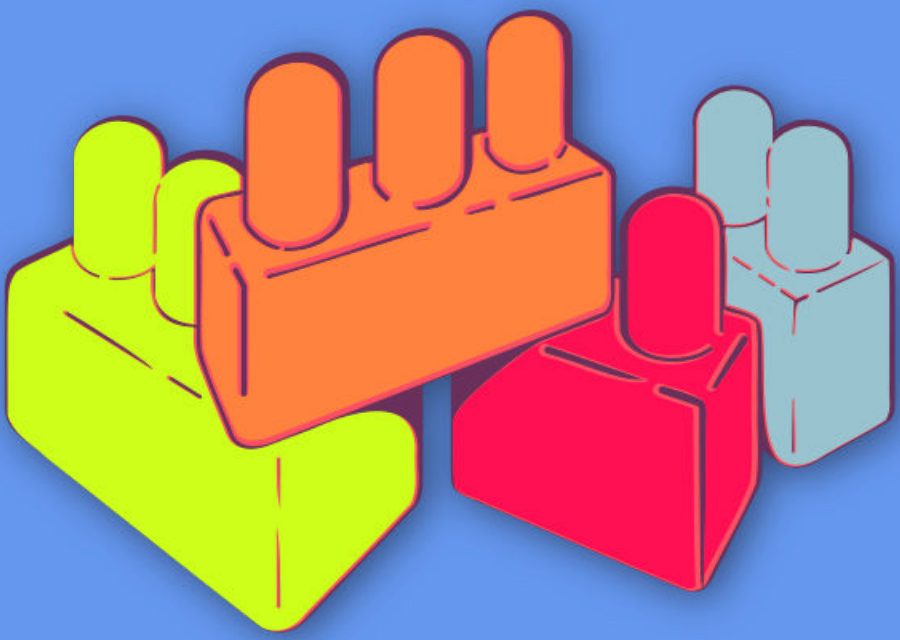
CIBERMUJERES



# Principios básicos de seguridad digital 1

Cómo hacer más segura tu computadora




https://iwpr.net/

# Índice general

# Cómo hacer más segura tu computadora

- **Objetivos:** Identificar buenas prácticas para mantener nuestras computadoras seguras.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - ¿Cómo funciona Internet?[1]
  - Navegación más segura[2]
  - Malware y virus[3]
  - Almacenamiento y cifrado[4]

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

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

[3] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-1/malware-y-virus/

[4] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-2/almacenamiento-

- **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

y-cifrado/

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[5]

    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

[5] http://www.osalt.com

software propietarios (por ej. Ubuntu vs. Windows; LibreOffice vs. Microsoft Office; Inkscape vs. Adobe Illustrator)

TechSoup[6]

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:

[6] http://www.techsoupglobal.org/network

- 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 su-

ficientemente 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