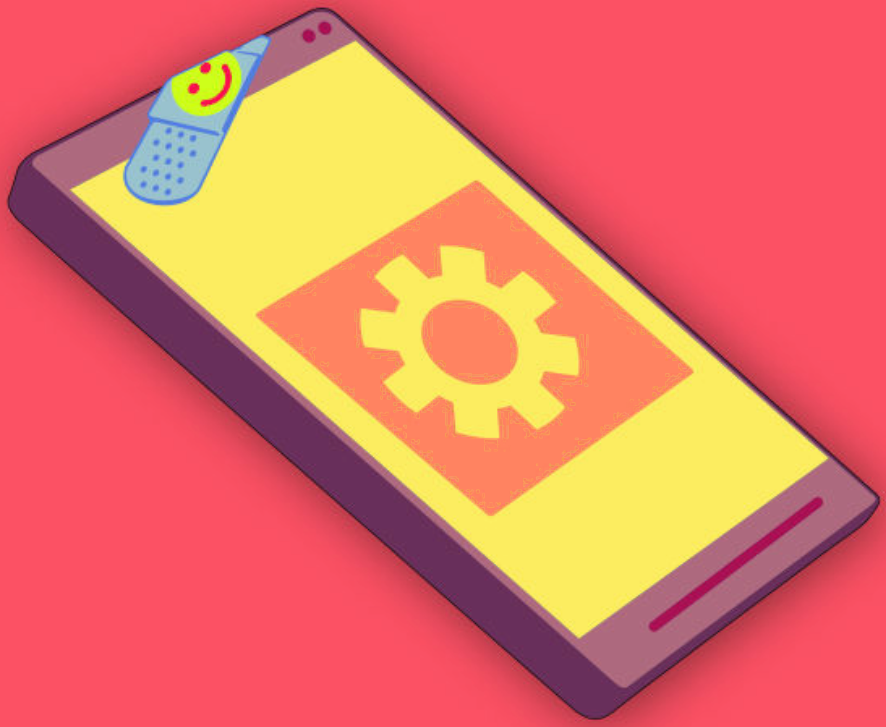
CIBERMUJERES



# Celulares más seguros

# Celulares más seguros




https://iwpr.net/

# Índice general

# Marco Polo

- **Objetivos:** Ideal para explicar cómo funciona un celular y cómo recibimos mensajes sms, llamadas y datos móviles en nuestros dispositivos.
- **Duración:** 15 minutos
- **Formato:** Ejercicio
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Multitudes interconectadas[1]
  - Campañas online más seguras[2]
- **Materiales requeridos:**
  - ¡Creatividad!

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

[1] https://cyber-women.com/es/privacidad/multitudes-interconectadas/

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

## 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

- **Objetivos:** Brindar un repaso introductorio de cómo funcionan los celulares y las redes de telefonía celular.
- **Duración:** 60 minutos
- **Formato:** Sesión
- **Habilidades:** Básico
- **Conocimientos requeridos:**
  - Ninguno requerido
- **Sesiones y ejercicios relacionados:**
  - Marco Polo[1]
  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[2]
- **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.

[1] https://cyber-women.com/es/celulares-más-seguros/marco-polo/
[2] https://cyber-women.com/es/privacidad/apps-y-plataformas-online/

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

## 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 Wi-Fi. 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

- **Objetivos:** Introducir herramientas y recomendaciones para mejorar la seguridad que tienen las participantes, ya familiarizadas con conceptos básicos de seguridad digital, con sus celulares.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Marco Polo[1]
  - Celulares Parte 1[2]
  - Introducción al cifrado[3]
  - Cómo hacer más segura tu computadora[4]
- **Sesiones y ejercicios relacionados:**
  - Marco Polo[5]
  - Celulares Parte 1[6]

[1] https://cyber-women.com/es/celulares-más-seguros/marco-polo/

[2] https://cyber-women.com/es/celulares-más-seguros/celulares-parte-1/

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

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

[5] https://cyber-women.com/es/celulares-más-seguros/marco-polo/

[6] https://cyber-women.com/es/celulares-más-seguros/celulares-parte-1/

  - Apps & Plataformas online: ¿Amigo/a o enemigo/a?[7]
  - Cómo hacer más segura tu computadora[8]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)
  - 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

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

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

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