MATERIAL DE CONSULTA: CELULAR (MÓVILES)

Material de consulta esencial para todos los talleres y actividades relacionadas con celulares (móviles).

Contenidos:

Materiales y referencias de consulta:

- Herramientas para celulares (Security in-a-box, Tactical Tech)
  https://securityinabox.org/es/android/

- Temario para facilitadoras: seguridad para celulares (Level-Up)
  https://www.level-up.cc

- App Umbrella para Android (Security First)
  https://play.google.com/store/apps/details?id=org.secfirst.umbrella&hl=es

1. Compara celulares

Cada tipo de celular tiene un conjunto específico de ventajas y desventajas Abajo mostramos una comparativa entre celulares Android, iPhone, Windows y celulares de baja gama.

Android

(Aclaración: no todas las versiones de Android son iguales en términos de funcionalidades y seguridad.)

Ventajas:

- *Open source*: El sistema operativo Android es *open source*.
- Puedes utilizar un catálogo de aplicaciones *open source* (tienda app): F-Droid.
- Hay buenas herramientas de seguridad por ahí: Psiphon, Panic button.
- Existen herramientas *open source* de comunicación más segura: Signal, Chatsecure.
- Tor: puedes conectarte a la red Tor a través de las herramientas Orbot y Orfox.
- Protección contra el malware: Android cuenta con múltiples capas de protección contra malware.
- Celulares robados o extraviados : Existen gestores de dispositivos para ayudarte a recuperar tu celular.

Limitaciones:
- El modelo de negocios de Google se basa en el uso de datos.
- Malware: aunque existan opciones para protegerse, sigue habiendo malware (por ejemplo, Androrat).

iPhone
Ventajas:
- Puedes habilitar un bloqueo de pantalla más robusto.
- Malware: hay menos malware en la "App Store" de iTunes que en el Play Store de Android.
- Se otorgan permisos por separado para cada aplicación.
- Existen herramientas *open source* de comunicación más segura: Signal, Chatsecure, Surespot
- Aplicación Buscar mi iPhone para celulares extraviados o robados.

Limitaciones:
- Código propietario.
- Comparado a Android, no existen muchas opciones de aplicaciones de seguridad.
- Por defecto, el bloqueo de pantalla es de solo cuatro a seis dígitos.
- Las llaves de cifrado se almacenan en los servidores de Apple.

Celular Windows
Limitaciones:
- Código propietario.
- No existen aplicaciones de seguridad.
- No puedes cifrar.

Celulares de baja gama
Limitaciones:
- Generalmente no puedes bloquear la pantalla.
- Código propietario.
- No puedes cifrar.

2. Criterios para un celular más seguro
Si quieres comprar un celular para implementar tantas medidas de seguridad como sea posible, aquí van unos criterios a tener en cuenta:

- Batería: comprueba que puedas sacar la batería.
- Actualizaciones: el fabricante del celular debe tener una buena reputación ofreciendo actualizaciones regularmente.
- Sistema operativo: comprueba la versión - ¿permite cifrar el celular? (versiones más viejas no lo permiten).

- Chipset (circuito integrado auxiliar): el chipset de MediaTek (MTK) es el único que te permite cambiar el número IMEI. Puedes encontrar una lista de dispositivos con este chip aquí: https://en.wikipedia.org/wiki/List_of_devices_using_Mediatek_SoCs

3. ¿Qué es un celular? Desglose en cuatrocapas.

Las siguientes anotaciones están diseñadas para complementar la serie de tarjetas "Desglose de celulares". Puedes descargarlas aquí: https://myshadow.org/materiaĺs

Página 1: "Núcleo"

- Banda base de IMEI: La banda base permite que se establezca una conexión entre el proveedor de telefonía celular y la infraestructura celular. El IMEI es un identificador único del celular y se conecta con la banda base. En la mayoría de los países es ilegal cambiar el número IMEI y, de hecho, en la mayoría de los celulares ni lo puedes hacer.

- Batería: ¿la puedes quitar? Esa es la única manera de realmente apagarla.

- Unidad Central de Procesamiento (CPU): cada vez hay más celulares que integran la banda base en el CPU en vez de mantenerlas separadas. Esta integración implica que el proveedor de telefonía celular puede acceder a tu CPU y el CPU, a su vez, puede acceder a la infraestructura celular (torres celulares y rastreo por geolocalización).

Página 2: "Inteligente"

- GPS: hay tres maneras en que pueden determinar tu ubicación: a través de la banda base, a través de torres celulares (la triangulación entre tres da con tu ubicación exacta), y a través de GPS, satélites o Wi-Fi.
- Wi-Fi: cuando el Wi-Fi está prendido, tu celular divulgará todas las conexiones Wi-Fi que conoce, es decir, publica el historial de todas las redes a las que se ha conectado tu celular en el pasado. A partir de esta información, también pueden predecir dónde vas a estar en el futuro.

- Tarjeta SIM: contiene tu número de celular. En muchos países, al registrar tu número de celular, tienes que asociarla a tu identidad legal, ya sea cuando compras la tarjeta SIM o a lo largo de las primeras semanas de utilizarla.

- Sensores de posición: ¿tu celular está tumbado sobre una superficie o está de pie? ¿Cambia la velocidad a la que se está moviendo? ¿O se está moviendo en alguna dirección específica? Pueden usar los sensores de posición para interpretar si alguien se está moviendo, hace una llamada o manda un mensaje de texto o si está durmiendo.

Página 3: "Sistema operativo"

- Aplicaciones integradas: vienen con tu celular y no las puedes borrar. Cuando actualizas tu celular, pueden instalarse nuevas aplicaciones integradas. En los celulares Android, puede haber aplicaciones integradas que no sean de Google sino del fabricante (Sony, Samsung, etc.).

- Sistema operativo: cada sistema operativo está desarrollado y es propiedad de una empresa distinta (Android = Google / iOS = Apple / Windows = Microsoft), y esto se traduce en ventajas y desventajas desde un punto de vista de privacidad y seguridad.

- Aplicaciones de terceros: son las que te instalas voluntariamente desde terceros.

- Tienda App: tu sistema operativo determina qué tienda de aplicaciones vas a utilizar. Android viene con Google Play Store, *iPhone* viene con Apple App Store. Ambas tiendas requieren de una cuenta de correo para funcionar. Ojo: si el correo que usaste para registrarte en tu tienda app también está vinculada a tu tarjeta de crédito, tu celular estará asociado a tus transacciones financieras. Sin embargo, las usuarias de Android pueden optar por F-Droid, una tienda de aplicaciones alternativa que no está relacionada con Google. Este catálogo de aplicaciones libres y *open source* no requiere que registres tus datos.

- *Aclaración:* lo anterior no aplica necesariamente a celulares que han sido *rooteados*.

Página 4: Rastros digitales

- Información financiera: la mayoría de las tiendas de aplicaciones están conectadas a una tarjeta de crédito, que está vinculado a su vez a tu nombre y cuenta bancaria.

- Correo: ¿qué cuenta de correo asociaste a tu tienda de aplicaciones? Tu proveedor de correo recibirá una notificación de cada aplicación que descargas o compras. Si tienes un iPhone y usas Gmail, estás compartiendo, de hecho, esa información con ambas empresas. Google puede relacionar tu actividad en su tienda de aplicaciones con tu perfil de Google.

- Fecha, hora y frecuencia: pueden utilizar los metadatos de fecha y hora (de tus archivos, llamadas, etc.), además de la frecuencia con la que estás en contacto con tu celular para analizar en conjunto estos datos (utilizando programas informáticos potentes) y revelar patrones en tus redes, relaciones sociales, ubicación, etc. Por ejemplo, imagínate que estás llamando a alguien: ¿es de día o de noche? ¿Cuánto tiempo te quedas hablando con la otra persona? ¿Cada cuánto la llamas? Las respuestas a esas preguntas pueden revelar si es tu pareja, amigo, compañera de trabajo, familiar, etc.

- Cuando se combina toda esa información con otros rastros digitales y las de otras personas, el retrato puede volverse increíblemente detallado.

4. Cómo se conecta tu celular a Internet

Cómo funciona Internet

EFF desarrolló un buen diagrama interactivo mostrando la infraestructura de Internet
https://www.eff.org/pages/tor-and-https

El diagrama también muestra quién puede ver qué en cada tramo y cómo varía según te conectes a Internet vía https o a través de Tor.

HTTP y HTTPS

- Cuando te conectas a un sitio web, la conexión entre tú y el sitio será a través de uno de los siguientes protocolos: http (por defecto) o https.

- Cuando te conectas vía https, se crea una conexión cifrada entre el sitio y tu celular. Cualquier dato que envías a través de esa conexión (correos, contraseñas, etc.) se hace un revoltijo y no puede ser descifrado por ninguna persona en el camino.

- Sin https(como cuando te conectas a través de http) tus datos, incluyendo tus contraseñas, viajan sin cifrar a través de la red y pueden ser vistos por terceros.

- Puedes comprobar que tu conexión utiliza https si aparece un candado verde a la izquierda de la URL. Si no hay candado verde, tus datos están viajando destapados.

- Generalmente, se aplica el protocolo https en sitios de bancos y tiendas en línea, en tu webmail, pero también en muchos otros sitios. Que un sitio web soporte una conexión https depende de la persona administradora, quien tiene que implementar el certificado https.

HTTPS Everywhere
https://www.eff.org/https-everywhere

Android: Puedes forzar conexiones vía https siempre que sea posible (que el sitio web tenga certificado y tu navegador soporte https) instalando el complemento HTTPS Everywhere en tu navegador Firefox. Este complemento encripta por defecto todas tus conexiones con los sitios web que navegas, siempre y cuando soporte https.

iPhone: HTTPS Everywhere no está disponible para Firefox en iPhone.

Tor
https://www.torproject.org/

- Puedes conectarte a Internet a través de la red Tor que permite que las usuarias escondan su dirección IP (y, por tanto, su geolocalización), bloquea rastreadores y fuerza conexiones HTTPS siempre que sea posible. De esta manera, puedes contar un cierto grado de anonimato en línea.

- Utilizando Tor, cuestiones legales y otros asuntos a considerar: En algunos países, usar Tor puede ser una señal de alarma o incluso ser ilegal. Según tu modelo de amenazas y riesgos, quizás Tor no sea la mejor opción para ti.

- "Sólo los criminales usan Tor:" activistas, disidentes y cualquier persona preocupada por su privacidad utilizan Tor también.

- Instalar Tor:
  - *Android:* instala la aplicación Orbot primero, que te conecta con la red Tor y después instala el navegador Orfox. Aprende más en el sitio de Guardian Project (desarrollaron Orbot y Orfox): https://guardianproject.info

  - *iPhone*: no puedes usar Tor en iPhone.

5. Comparación de navegadores en celulares

Android
(ten en cuenta que todos los navegadores descritos a continuación funcionan junto con Orbot).

Firefox para Android
Desarrollado por Mozilla

Ventajas:
- Personalizar: En Android, Firefox es el único navegador donde puedes cambiar las configuraciones de privacidad por defecto e instalar complementos.

- Demuestra su compromiso hacia la seguridad e invierte una buena cantidad de dinero en resolver bugs y detectar errores en su software.

- Revocación de certificados SSL: los maneja mejor que cualquier otro navegador.

- La protección de datos es un punto clave: su manifiesto corporativo afirma que "la seguridad y privacidad de los individuos en Internet son fundamentales y no deben ser tratadas como opcionales."

- El código fuente está disponible (Firefox es el único navegador que pone a disposición su código completo).

- Sin ánimo de lucro: Firefox es desarrollado por Mozilla, una organización sin ánimo de lucro que produce software libre gratuito de alta calidad. Esto significa que el navegador no es parte de un modelo de lucro.

- Nueva Ventana Privada: modo de navegación fácil de usar que impide Firefox guardar tu historial de navegación y ofrece una protección parcial contra rastreadores.

Limitaciones:
- Aún no brinda la seguridad que ofrece Chrome.

Chrome para Android
Desarrollado por Google

Ventajas:
- Seguridad: Chrome es de los mejores navegadores en este sentido.

- Flash está integrado y automáticamente actualizado, lo que implica que se minimizan las vulnerabilidades (ojo: las auditorías de seguridad de Chrome fueron fundadas por Google en 2011 y mucho ha cambiado desde entonces).

- Modo incógnito": modo de navegación fácil de usar que impide Chrome guardar tu historial de navegación.

Limitaciones:
- Privacidad: Google genera la gran parte de su dinero a través de publicidad. Para ello, utilizan información que recopilan a través de sus servicios, incluyendo Chrome: averiguan qué haces, dónde estás, qué compras, etc.

- Configuración por defecto: en Android, las personas usuarias no pueden cambiarla.

- No es *open source*.

Orfox para Android.
Desarrollado por The Guardian Project. Orfox funciona junto con Orbot. Tienes que instalar primero Orbot y después, cuando vayas a utilizar Orfox, prende primero Orbot que se encarga de conectarse con la red Tor.

Ventajas:
- Privacidad: Orfox corre por defecto sobre Tor así que puedes tener anonimato en línea (esconde tu dirección IP) y bloqueo rastreadores

- Evasión: ayuda a las usuarias evadir la censura en línea.

Limitaciones:
- Quizás no puedas utilizar todos los servicios en línea.

iPhone

Safari para iPhone
Desarrollado por Apple

Ventajas:
- Personalización: Safari es el único navegador en iPhone donde puedes cambiar las configuraciones de privacidad por defecto.

Firefox para iPhone

Desarrollado por Mozilla

Ventajas:

- Demuestra su compromiso hacia la seguridad e invierte una buena cantidad de dinero en resolver bugs y detectar errores en su software.
- Revocación de certificados SSL: los maneja mejor que cualquier otro navegador.
- La protección de datos es un punto clave: su manifiesto corporativo afirma que "la seguridad y privacidad de los individuos en Internet son fundamentales y no deben ser tratadas como opcionales."
- El código fuente está disponible (Firefox es el único navegador que pone a disposición su código completo).
- Sin ánimo de lucro: Firefox es desarrollado por Mozilla, una organización sin ánimo de lucro que produce software libre, gratuito y de alta calidad. Esto significa que el navegador no es parte de un modelo de lucro.
- Nueva Ventana Privada: modo de navegación fácil de usar que impide Firefox guardar tu historial de navegación y ofrece una protección parcial contra rastreadores.

Limitaciones:

- Aún no brinda la seguridad que ofrece Chrome.
- No hay complementos disponibles - Firefox en iPhone en realidad es simplemente el navegador Safari envuelto en el caparazón de Firefox.
- No se pueden cambiar la configuración por defecto en iPhone.

Chrome para iPhone

Desarrollado por Google

Ventajas

- Seguridad: Chrome es de los mejores navegadores en este sentido.
- Flash está integrado por defecto y se actualiza automáticamente, lo que implica que se minimizan las vulnerabilidades (ojo: las auditorías de seguridad de Chrome fueron fundadas por Google en 2011 y mucho ha cambiado desde entonces).
- "Modo incógnito": modo de navegación fácil de usar que impide Chrome guardar tu historial de navegación.

Limitaciones:

- Privacidad: Google genera la gran parte de su dinero a través de publicidad. Para ello, utilizan información que recopilan a través de sus servicios, incluyendo Chrome: averiguan qué haces, dónde estás, qué compras, etc.
- No se puede cambiar la configuración por defecto.
- No es *open source*.

6. Buscadores

Alternativas a Google Search o Bing que respeten tus derechos de privacidad:

- DuckDuckGo - https://myshadow.org/duckduckgo
- Searx - https://myshadow.org/searx
- StartPage - https://myshadow.org/startpage

7. Cifra tu celular

Mientras los modelos más nuevos de iPhone cifran el celular por defecto en cuanto le aplicas una contraseña, las usuarias de Android tienen que hacerlo manualmente. T**en en cuenta que el proceso de cifrar tu celular requiere de una contraseña**; si la olvidas, no podrás acceder a tu celular nunca más. Así que, **antes de cifrar**:

- **Respalda todos los datos importantes** que están en tu celular: lista de contactos, fotos, videos, etc.
- **Carga la batería de tu celular** para que no se interrumpa el proceso de cifrado (lo que podría implicar una desconfiguración irreversible).
- **Utiliza una contraseña segura** para cifrar tu celular y asegúrate de recordarla.

8. Rastreo por geolocalización

Funciona principalmente de tres maneras

- **Wi-Fi:** cuando utilizas Internet via Wi-Fi, pueden rastrear tu ubicación por medio de tu dirección IP.
- **Datos de tu celular:** tu celular está constantemente conectándose a torres celulares en el área, cada una de ellas tiene una ubicación precisa. La triangulación de las torres celulares permite que sepan exactamente donde estás.
- **GPS:** el GPS integrado en tu celular habilita un rastreo de precisión (de parte de EEUU o Rusia – países dueños de los satélites GPS -, según el tipo de GPS que tenga tu celular).

9. Aplicaciones 'Busca mi celular' / 'Anti-robo'

¿Deberías utilizar una aplicación que te ayude a localizar tu celular en caso de robo o extravío?

- **Puedes utilizar una aplicación 'Busca mi celular' para:**
  - **bloquear** tu celular
  - **buscarlo** si lo perdiste o te lo robaron
  - **hacer que el celular suene** o haga ruido
  - **borrar los datos** del celular
- **Que decidas utilizar una de estas aplicaciones depende de cómo respondas a las siguientes preguntas:**
  - ¿Realmente te sería útil? ¿Cuáles son los riesgos de que roben tu celular?
  - ¿Cuál sería el impacto?
  - ¿Estás dispuesta a invertirle tiempo y energía? (descargar la aplicación, registrar el celular, aprender cómo funciona, probarlo).
  - ¿Confiarías el acceso a tus datos a las personas que desarrollaron la aplicación?

Si te decides por instalar una aplicación del tipo 'busca mi celular', recomendamos que utilices Avira

(http://www.avira.com/).

10. Aplicaciones

Aunque las aplicaciones estén "verificadas" por los dueños de las tiendas de aplicaciones (Google o Android), en realidad eso brinda muy poca protección ante lo que pueden hacer las aplicaciones una vez que las instalas en tu celular: algunas aplicaciones pueden, por ejemplo, copiar y enviar tu directorio de contactos. Sin embargo, generalmente puedes recuperar parte del control sobre lo que tu aplicación puede o no puede hacer y a qué partes del celular accede.

Acceso necesario

A veces ciertos accesos son requeridos para que la aplicación pueda funcionar, por ejemplo, muchas aplicaciones de mensajería (como Whatsapp y Signal) necesitan acceder a tu lista de contactos. Si te incomoda que tenga este tipo de permisos, reconsidera el hecho de instalarla.

Permisos

- Comprueba qué tipo de acceso tienen las aplicaciones instaladas en tu celular: ubicación, contactos, fotos, calendario, altavoces, micrófono, cámara.

- Limita los permisos de acceso cuando sea posible. Si una aplicación requiere de más acceso que la que estás dispuesta a otorgar, piensa dos veces si instalarla o elimínala si ya la tienes. Quizás existan mejores alternativas o ni si quiera necesitas ese tipo de aplicaciones realmente.

Permisos "excesivos"

¿Tu aplicación de lector de noticias accede a tus contactos? ¿La aplicación de navegación y mapas que recién instalaste quiere acceder a tus fotos? ¿Por qué? Como este tipo de permisos no son indispensables para que la aplicación funcione, puedes negarlas. Si no puedes, considera utilizar aplicaciones alternativas con accesos y condiciones más apropiadas.

Tienda de aplicaciones / Play Store

Registro de actividad: toma en cuenta que, en la medida que necesites iniciar sesión para instalar una aplicación de App Store o Play Store, Google o Apple tienen un registro de todo lo que buscas, descargas e instalas.

Tiendas app alternativas

Android

- Si quieres salirte de Google Play Store, existen alternativas, por ejemplo, F-Droid o la tienda de aplicaciones de Guardian Project. Ambas ofrecen aplicaciones libres y *open source*. En general, revisa si confías en el sitio web de la aplicación antes de descargarla.
- Necesitas configurar tu celular adecuadamente para instalar herramientas de una tienda de aplicaciones que no sea Google Play.

iPhone

- No puedes salirte de la tienda App Apple.

Cómo verificar si una aplicación es confiable

- Comprueba la firma gpg de la aplicación. Por defecto, Android requiere que todas las apps estén firmadas con una firma gpg. De esta manera, puedes identificar a las personas desarrolladoras de la aplicación (ej. verificar si es confiable y legítimo), además de establecer una relación de confianza entre las aplicaciones que tienen la misma firma. *Ejemplo*: esta es la firma de la app Orbot en F-Droid: https://f-droid.org/repo/org.torproject.android_15012316.apk.asc

- Realiza múltiples descargas: una de las formas más fáciles de verificar una firma es descargando la

aplicación varias veces desde diferentes lugares, dispositivos y sitios web y comparar las firmas entre sí para asegurarte que sea la misma y pertenezcan al mismo grupo de personas desarrolladoras.

- Comparar firmas gpg. Este método es un poco más difícil. En esta guía puedes encontrar los pasos necesarios: https://www.gnupg.org/download/integrity_check.html

- Chekey es una aplicación desarrollada por Guardian Project que te ayuda a verificar apps: https://play.google.com/store/apps/details?id=info.guardianproject.checkey

11. *Rootear* / *Jailbreakear* tu celular

¿Deberías *rootear* tu celular Android o *jailbreakear* tu iPhone? La respuesta sencilla es seguramente no :)

- *Rootear* significa que tienes acceso *root* a tu dispositivo. Es como ejecutar programas como una administradora en tu computadora Windows.

- *Rootear* también implica desbloquear tu sistema operativo, lo que te permite eliminar aplicaciones integradas en tu celular e instalar un sistema operativo alternativo o aplicaciones que no son aprobadas por Google/Apple o el fabricante de tu celular.

- Aclaraciones con respecto a jurisdicciones: en algunos lugares, *rootear/jailbreakear* es ilegal.

- Ojo que la mayoría de las herramientas para *rootear* provienen de China y potencialmente contienen malware. Si decides *rootear* tu celular, es importante que utilices una herramienta de confianza como Superuser disponible en F-droid.
  https://f-droid.org/repository/browse/?fdcategory=Security&fdid=me.phh.superuser&fdpage=2

Lo bueno de *rootear/jailbreakear*

Puedes eliminar aplicaciones integradas que no utilizas: ahorras espacio y batería.

- Permisos: si usas un Android 5 o más viejo, puedes instalar una aplicación para controlar los permisos de las aplicaciones.

- Actualizaciones: puedes instalar un ROM personalizado para conseguir las últimas actualizaciones de Android, generalmente atrasadas o bloqueadas por tu fabricante de celular.

- Seguridad: obtienes control total sobre las configuraciones de privacidad y seguridad de tu celular.

Lo malo de *rootear/jailbreakear*

- Riesgos: puedes dejar tu celular inservible (*'bricking'*: convertirlo en un ladrillo).

- Anulación de garantía: posiblemente se anule la garantía que tengas con el fabricante o el proveedor.

- No hay vuelta atrás: el proceso es potencialmente irreversible.

Tomando todo lo anterior en cuenta, si quieres rootear tu celular, puedes consultar los siguientes materiales:

- http://www.cyanogenmod.org
- https://wiki.cyanogenmod.org/w/P760_Info
- https://es.wikipedia.org/wiki/Replicant_(sistema_operativo)

12. Pasos para sesiones prácticas - Android & iPhone
Pasos básicos

1. Cuenta de correo

Tu celular siempre se vincula con una cuenta de correo principal que está asociada, a su vez, a tu tienda de aplicaciones / cuenta Play Store. Si creas una cuenta de correo específicamente para tu celular, potencialmente estás limitando que mapeen tus relaciones sociales ("*social graphing*") y contribuye a compartimentar tus rastros digitales.

- *Android*: Android requiere de una cuenta de correo Gmail; sin embargo, puedes crear una nueva cuenta de correo exclusivamente para tu celular y cuenta Google Play. De esta manera, dificulta que Google asocie tus diferentes redes sociales.

- *iPhone*: preferiblemente no uses una cuenta Gmail.

2. "Nombre" de celular

Cámbiale el nombre a tu celular a algo que no esté relacionado con tu identidad (por ejemplo, tu nombre). Si alguien escanea la red cercana de dispositivos, este nombre estará visible.

3. Contraseñas

- Configura una contraseña fuerte y segura para tu celular.

- Crea contraseñas diferentes para cada aplicación siempre que puedas.

- Deshabilita la opción de visualizar las contraseñas cuando la estás tecleando.

4. Cifra el celular

Véase anotaciones sobre "Cifrado" en la sección siete de este documento. Mientras los modelos más nuevos de iPhone cifran el celular por defecto en cuanto le aplicas una contraseña, las usuarias de Android tienen que hacerlo manualmente. No recomendamos que hagas esto en una sesión práctica porque las participantes pueden olvidar su contraseña. Sin embargo, puedes mostrarles dónde está la opción para que lo hagan con calma, enfatizando que respalden sus datos antes, asignen una contraseña segura y revisen que su celular tenga la batería cargada.

5. Bloquea tu tarjeta SIM

Configuración

6. Respaldo & Reseteo

Android:

- Respaldo: tienes la opción de no respaldar tus datos en los servidores de Google.

- Reseteo: además, en la opción de "reseteo de fábrica", puedes resetear tu celular y borrar todos tus datos desde la memoria interna.

iPhone:

- Respaldo: puedes optar por no respaldar tus datos en el iCloud de Apple o realizar un respaldo parcial: Configuración > iCloud > Asigna permisos a cada ítem que quieras compartir en tu iCloud. (Puedes transferir manualmente fotos desde tu celular a tu computadora a través de un cable).

- Reseteo: puedes resetear tu celular y borrar todo el contenido adentro desde la opción: Configuración >

General > Reseteo.

7. Números (identificadores) únicos
Aprende dónde encontrar los números (identificadores) únicos de tu celular (IMEI, SIM, etc). Esto puede ser útil si roban tu celular.

Conectividad & rastreo

8. Wi-Fi
Deshabilita tu Wi-Fi cuando no lo estás usando. Cuando el Wi-Fi está prendido, tu celular divulgará todas las conexiones Wi-Fi que conoce, es decir, publica el historial de todas las redes a las que se ha conectado tu celular en el pasado.

9. Bluetooth
Apaga tu Bluetooth cuando no lo estás usando.

10. Limita el rastreo por ubicación
- Apaga tu celular y sácale la batería cuando sea posible. Si quieres bloquear este rastreo 100%, simplemente deja tu celular en casa o usa una bolsa/jaula de Faraday.
- Pon tu celular en modo avión cuando no necesitas estar conectada.
- Cambia configuraciones:

Android:
- Deshabilita rastreo por ubicación. (Ten en cuenta que implicará deshabilitar algunos servicios como determinadas funcionalidades de Google Maps.) Configuración de Google > Servicios > Ubicación
- Borra tu historial de ubicación: Configuración de Google > Servicios > Historial de ubicación de Google.

iPhone:
- Apaga los servicios de ubicación: Configuración > Privacidad > Servicios de ubicación > apagar

11. Salte de "Publicidad basada en intereses"
Android: Configuración de Google > Servicios > Publicidad: habilita la opción que no quieres recibir publicidad basada en tu perfil de intereses. Esto le indicará a tus aplicaciones no utilizar tu ID de publicidad (identificador utilizado para construir perfiles de usuaria o mostrarte publicidad personalizada). Después puedes resetear tu ID de publicidad marcando la opción "Resetear/reestablecer ID de publicidad".

iPhone: configuración > Privacidad > Publicidad > habilita "Limitar seguimiento"

12. Escoge y personalizar tu navegador
Compara los navegadores disponibles para tu sistema operativo y escoge uno para que sea tu aplicación de navegación por defecto.

*Android:*Instala y personaliza Firefox. *(En Android, Firefox es el único navegador donde puedes cambiar las configuraciones de privacidad por defecto e instalar complementos).*
- Cambiar de buscador
- Bloquear ventanas emergentes
- Habilitar opción "No rastrear"
- Borrar historial y datos en el caché de los sitios web.
- Instalar HTTPS Everwhere

iPhone: Safari (Safari es el único navegador para iPhone donde puedes cambiar la configuración por defecto: Configuración > Safari):

- Cambiar el buscador
- Bloquear ventanas emergentes
- No rastrear
- Borrar historial y datos en el caché de los sitios web.
- El historial de navegación está almacenado en Configuración > Safari > avanzado > datos de sitios web

13. Cambia la manera en que te conectas a Internet

Configura VPN o Tor (sólo puedes utilizar Tor en Android).

Android: Instala Orbot y Orfox

- Para usar Orfox, primero tienes que instalar Orbot. De esta manera, podrás conectarte a la red Tor. Puedes instalar tanto Orbot como Orfox directamente en Google Play, F-droid o el Guardian Project.

- Orbot: guía práctica: https://securityinabox.org/es/guide/orbot/android/

- Orfox y Orbot: Más información: https://guardianproject.info/2015/06/30/orfox-aspiring-to-bring-tor-browser-to-android/

iPhone: como Tor no está disponible en iPhone, para una navegación más segura es recomendable que configures una VPN y dirijas tu tráfico por ahí.

- Escoge un proveedor VPN, como por ejemplo iPredator, RiseUp VPN, o Tunnelbear.

- Configura la VPN en tu celular: Configuración > General > VPN > Agrega configuración de VPN--> agrega las configuraciones de tu elección de proveedor de VPN y tu cuenta de usuaria.

- Para comprobar que tu VPN está habilitada: Configuración > verifica si está la VPN encendida.

Seguridad & Permisos

14. Instala un antivirus.

Recomendamos Avira (te permite localizar tu celular si lo extraviaste o te lo robaron).

15. Busca mi celular

El anti-virus Avira te permite buscar tu celular o puedes también:

- si tienes *Android*, puedes descargar el Gestor de dispositivos desde el Play Store

- si tienes *iPhone*, puedes utilizar la app "Busca mi iPhone".

16. Verifica y limita los accesos y permisos que tienen tus aplicaciones

Android:

- En versiones más nuevas de Android, puede aplicar permisos por aplicación. Considera limitar el acceso a: ubicación, contactos, fotos, micrófono, cámara, calendario

- Anotación: en versiones más viejas de Android, sólo puedes aplicar permisos generales a través de la sección 'Google' en configuración.

- Control de actividad: Configuración de Google > Cuenta > Información personal & privacidad > Control de actividad > deshabilitar:
  - Historial de búsqueda de YouTube
  - Historial de reproducción de YouTube
  - Historial de ubicación de Google.

iPhone:
Puedes comprobar y administrar los permisos de tus apps en la configuración:
Configuración > Privacidad > limitar acceso por app a lo siguiente:
ubicación, contactos, fotos, micrófono, cámara, calendario.

17. Habilita la instalación de aplicaciones de fuentes desconocidas
Sólo posible en Android: te permite descargar aplicaciones que no sean de Google Play Store.

18. Evaluar tus aplicaciones
- Reducir: ¿realmente utilizas todas tus aplicaciones? ¿Cuáles podrías borrar?

- Escoge aplicaciones que respeten tu privacidad. Revisa las aplicaciones que están en tu celular. ¿Por qué decidiste instalar específicamente esas aplicaciones? ¿Lo hiciste porque te lo pidió una amiga? ¿O fue una decisión tuya? Conversa sobre qué hace que una aplicación sea más segura y respete más tu privacidad (que sea *open source*, use cifrado, quiénes son los dueños/desarrolladores, dónde está ubicada la empresa, a qué datos solicita acceso, te permite utilizarlo bajo un pseudónimo o anónimamente, etc.) Encuentra más información en https://myshadow.org.

13. Pasos para una sesión práctica - Celulares de baja gama
(Un celular de baja gama es un celular básico que no tiene acceso a Internet)

- Configúrale un código pin o, si el celular te deja, una contraseña más larga.

- Sácale la batería para protegerte del rastreo por geolocalización y la intercepción de tus comunicaciones.

14. Estrategias para la Resistencia: enfoque en celulares (o móviles)

A continuación, encontrarás ejemplos orientados a celulares. Se pueden clasificar según cuatro tipos de estrategias de resistencia. Para una explicación más detallada de cada categoría y más ejemplos, descarga el material de consulta "Estrategias para la Resistencia" en myshadow.org/materials.

Reduce
- Apaga los servicios que no estás utilizando (Wi-Fi, Bluetooth, etc.).
- Pon tu celular en modo avión.
- Elimina las aplicaciones que ya no utilizas.
- Cambia los permisos de tus aplicaciones.

Compartimenta
- Utiliza diferentes aplicaciones de mensajería para diferentes redes sociales.
- Utiliza diferentes navegadores para diferentes cosas.
- Utiliza una nueva cuenta de correo electrónico como tu correo principal (no la cuenta que usas cada día).

MATERIAL DE CONSULTA: CELULAR (MÓVILES)

Ofusca

- Utiliza una VPN, cambia el nombre de tu celular.
- Crea contactos falsos en tu celular.
- Deja tu celular en casa a veces, oculta a dónde vas y rompe tu rutina.

Refuerza

- Configura un cifrado de disco completo si no está hecho automáticamente (cifra tu celular).
- Ponle una contraseña a tu celular.
- Establece contraseñas en aplicaciones específicas.
- Instala la aplicación Busca mi iPhone.