

Anexo 3. Insumos entregados con recomendaciones en los talleres

Protección frente al acceso físico

Garantizar en la mayor medida posible que la información del teléfono no sean accesibles a terceros, en el caso de que lo tuvieran físicamente

Desbloqueo seguro

Se puede proteger el teléfono con patrones, pines, contraseñas o datos biométricos. ¿Cuál es el más seguro? Depende de ti.

Patrón de desbloqueo

Algunas características que disminuyen su eficacia: (1) se puede seguir el patrón con la grasa que dejan nuestros dedos en la pantalla, (2) es sencillo averiguar viendo encima del hombro y (3) los patrones se pueden repetir

PIN numérico

Tiene la desventaja de tener menos opciones

Contraseña

Tiene la ventaja de tener más opciones (mayúsculas, minúsculas, números y símbolos), pero es más difícil de recordar.

Desbloqueo biométrico

Es algo que somos, no algo que sabemos, a diferencia de las otras opciones. Una desventaja es que se nos puede obligar sin nuestro consentimiento con el uso de la fuerza.

Protección frente al acceso físico

Filtración de información a través de la pantalla o altavoces

A veces ciertas configuraciones predeterminadas pueden hacer muy sencillo que la persona a un lado o con nuestro celular vea o escuche información nuestra, sin desbloquearlo.

- Asegurar que las notificaciones solo se puedan ver cuando está desbloqueado el celular. Desactiva que aparezcan sin estar desbloqueado el celular.
- Disminuir el brillo de la pantalla al poner nuestro PIN, contraseña o patrón de desbloqueo. También se puede comprar una pantalla de privacidad, que es un plástico polarizado que se pone sobre la pantalla, permitiendo que solo la persona que tiene el celular delante pueda leerlo.
- Desactivar asistentes de voz que permiten usar el telefono sin que esté desbloqueado.

A la hora de protegernos, necesitamos preguntarnos, ¿de qué me estoy protegiendo?

Debemos considerar que puede hacer nuestro adversario:

- *¿Puede observarme desbloquear el teléfono antes de ganar acceso físico a él?*
- *¿Puede obligarme o coaccionarme para desbloquear el dispositivo?*
- *¿Puede recoger muestras biométricas (huellas, iris, fotografías) para desbloquear el celular?*

Si la respuesta es sí a estas preguntas, la mejor opción es utilizar las opciones más seguras de lo previamente visto (por ejemplo, una buena contraseña que se cambie regularmente).

Comunicaciones seguras

Los teléfonos son primordialmente para comunicarnos. Es importante considerar si otros remotamente tienen acceso a las comunicaciones:

¿Puede otro ver mis mensajes, escuchar mis llamadas? ¿Puede intervenir cuando visito una página web?

- *Navegación web: HTTPS*

- Toda información que se manda en una página con HTTP se manda sin protección, se puede ver y cambiar por otras personas.
- Las páginas con HTTPS cuidan la información que se manda, a través del cifrado, que cuida la confidencialidad.

- *Redes no confiadas: VPN*

- Si nos conectamos en redes wifi en lugares públicos, no sabemos si hay personas atacantes cercanas.
- Podemos usar una VPN, que es una red que nos cuida, con el cifrado de la información que se manda y recibe.

- *Comunicación instantánea*

- Los SMS y las llamadas también pueden ser intervenidas.
- Lo mejor frente es usar aplicaciones que cifran de extremo a extremo en los mensajes y llamadas. Es una medida de protección en que solo el celular que manda y el celular que recibe puede leer o ver la información enviada.
- Una aplicación que cifra nuestra información es Signal.

- *Contraseñas y 2FA*

- Escoger nuestras contraseñas es importante. Son como la ropa interior: no las reutilices, no las compartas y no las dejes a la vista.
- Debe ser secreta y robusta: no uses información como fechas, nombres o lugares. Escoge frases o palabras al azar.
- El mejor modo es no tener que recordarlas, utilizando un gestor de contraseñas.

Protección de la privacidad

Gran parte de la información que tenemos en nuestro celular puede ser accedida por muchas aplicaciones.

¿De dónde viene / de quién es la aplicación?

Un punto importante para evitar que alguien tenga acceso remotamente sin nuestro conocimiento es instalar aplicaciones de proveedores fiables y mantenerlas siempre actualizadas.

- *Canales de distribución de aplicaciones*
 - Google Play Store y F-Droid en Android | App Store en Apple
 - *Nunca debemos instalar aplicaciones de fuentes desconocidas.*
- *Actualizaciones*
 - Las actualizaciones son importantes para solucionar problemas de seguridad que se van descubriendo con tiempo.
- *Control de permisos*
 - En los ajustes o configuración de nuestro celular, podemos ingresar a las aplicaciones y ver todas las que están instaladas. Para gestionar los permisos de cada aplicación, pulsamos sobre ella y luego sobre *Permisos*. Aquí podemos consultar qué permisos están activos y denegar o permitir los que queramos.

Navegación y privacidad

Para navegar, se recomienda usar un explorador con licencia libre, que sea respetuosa de nuestra privacidad.

- Firefox y DuckDuckGo son dos navegadores que son respetuosos con nuestra privacidad.
- Podemos complementarlos con otras extensiones o programas que nos apoyan en cuidar nuestra privacidad.

Redes sociales

Las redes sociales tienen un impacto grande en nuestra sociedad actualmente. Nos expone de distintas maneras, a través de nuestros datos personales, sino también en como las usamos.

Podemos tomar algunas medidas para cuidar más nuestro uso, pero no hay manera de evitar que las empresas tengan control sobre nuestros datos si usamos estas redes sociales.

la "f" azul

Facebook recopila y guarda una enorme cantidad de datos de las personas que lo usan. También se utiliza mucho para acosar, robo y extorsiones. Podemos tomar algunas medidas para protegernos un poco más al usar la red:

Fortalece tu contraseña

- Activa la verificación en dos pasos. Es una capa extra de seguridad. Se puede activar a través de SMS.

Puedes revisar en que dispositivos está abierta tu cuenta

- Esto lo puedes revisar en: Cuenta Configuración y privacidad Configuración Seguridad e inicio de sesión Dónde iniciaste sesión
- Cierra la sesión de forma remota: Cuenta Configuración y privacidad Configuración Seguridad e inicio de sesión Configurar seguridad adicional

Para no aparecer en los motores de búsqueda, como Google

- Elige "No" en la opción ¿Quieres que los motores de búsqueda fuera de Facebook enlacen a tu perfil?

Cambia la configuración para decidir quien puede ver tu actividad, escribir en tu muro, enviarte mensajes y etiquetarte:

Cuenta Configuración y privacidad Configuración Privacidad
Tu actividad

Redes sociales

El teléfono verde

WhatsApp no es una red social como tal, sino una aplicación de mensajería instantánea, de las más utilizadas en el mundo. Unos elementos para mejorar tu seguridad en su uso:

Ajustes de privacidad

Ajustes > Cuenta > Privacidad

- Ajusta los aspectos de privacidad como hora de última conexión, foto de perfil, ubicación en tiempo real y estado
- Cifrado punto a punto por defecto
- Activar notificaciones de seguridad
- Verificación en dos pasos
- Siempre puedes decidir lo que compartes con tus contactos en WhatsApp y por eso te recomendamos que tengas precaución antes de enviar contenido. Hazte esta pregunta: "¿Me importaría que otras personas vieran lo que voy a enviar?"

Para que tanto grupo

- Desactiva tus ubicaciones en tiempo real
- Cómo reaccionar ante comentarios con los que no estoy de acuerdo
- Eres visible para mucha gente ahí
- Spam
- Reenvío y réplica de información e imágenes

Alternativas:

- Puedes buscar alternativas que te hacen menos vulnerable a venta de datos y ataques en la red. Como mensajeros con opciones secretas y encriptadas:
 - Signal
 - Wire

Antenas falsas



¿Qué son?

Simula ser una torre de telefonía móvil y "engaña" a los celulares cercanos, interceptando la señal.

¿Qué pueden hacer?

- Conocer la ubicación geográfica del celular
- Interceptar SMS
- Enviar SMS falsos
- Editar SMS
- Interceptar llamadas. Las llamadas escuchadas son grabadas
- Realizar llamadas falsas
- Conocer los números de teléfono de los mensajes y las llamadas
- Prender el micrófono del celular para escuchar
- Bloquear la comunicación del celular

Escáner para extracción de información



¿Qué son?

Son tecnologías que permiten sacar de un celular toda la información propia y de otras, con el uso de escáneres.

¿Qué pueden hacer?

Pueden tener acceso a:

- registros de llamadas
- mensajes de SMS
- imágenes, vídeos, archivos de audio

Puede clonar chips, extraer contraseñas y recuperar información borrada, inclusive de contenido de comunicaciones en aplicaciones de mensajería como WhatsApp.

Drones



¿Qué son?

Son aviones pequeños que se puede utilizar para vigilar movimientos desde la distancia.

Se han utilizado mucho para la vigilancia en fronteras a nivel mundial, incluido por el INM.

¿Qué pueden hacer?

Vigilar en tiempo real desde las alturas, con personas a distancia monitoreando las imágenes/el video.

Existen drones que tienen tecnología de reconocimiento facial.

Revisión de celulares



¿Qué son?

La revisión física de los celulares por parte de distintos actores, en situaciones que son difíciles de resistir.

¿Qué pueden hacer?

La revisión de los celulares en los retenes son de las formas de intimidación y de extracción de información más común en la frontera sur.

Pueden acceder a la información que tenemos en nuestros celulares, poniendonos a nosotras y a otras en riesgo de ser información sensible.



Llamadas y señal

¿Cuales son los riesgos?

Intervención de llamadas, donde se puede tener información sensible sobre el contenido de la llamada, mi ubicación, información sobre la persona con la que hablo y acceso al microfono del celular.

¿Cómo me puedo proteger?

- Cuidar mi entorno - quien me esta escuchando alrededor.
- Considerar que información es absolutamente necesaria compartir en llamada y si tengo otra manera de comunicarme para compartir información sensible.
- Usar aplicaciones de mensajería cifradas. Recomendamos la aplicación de Signal.



Signal es una aplicación cuidadosa con la privacidad de las personas que la usan, que cifra las comunicaciones. Es gratuita y se pueden mandar mensajes, hacer llamadas y videollamadas. Está disponible en la PlayStore



Movilizaciones & Retenes

¿Cuales son los riesgos?

Al pasar por retenes, se enfrenta al riesgo de la revisión en físico de los celulares o el uso de escaners para extraer información. Esa información queda con las personas y grupos que revisan el celular, lo cual nos puede poner en riesgo a nosotras y nuestras redes.

¿Cómo me puedo proteger?

- Borrar información de mi celular. ¿Cuál información me puede poner en riesgo a mi y a otras personas si acceden actores agresores?
- Entregar el celular - no entregarlo puede poner en mayor riesgo nuestra seguridad física en el momento.
- Para información que es muy sensible, pero necesaria trasladar, recomendamos el uso de la aplicación Tella.



Tella es una aplicación que fue creada para personas defensoras de derechos humanos y periodistas. Es gratuita y permite guardar y "camuflajear" archivos - audios, imagenes, videos, textos - en el celular. Esta en la PlayStore.