Seguridad en dispositivos móviles

Cómo proteger celulares y tablets frente a los riesgos actuales.

Tu celular guarda casi todo

Los celulares y las tablets concentran comunicaciones, fotos, contactos, contraseñas, información laboral y datos financieros. Por eso, proteger el dispositivo, las cuentas y las aplicaciones es clave para evitar accesos no autorizados, fraudes y pérdida de información.

Principales riesgos

Apps maliciosas	Pueden intentar acceder a tu información, espiar tu actividad, mostrar publicidad engañosa o controlar funciones del equipo.
Phishing y smishing	Mensajes por correo, SMS o apps de mensajería que buscan robar contraseñas, datos personales o dinero con enlaces y pedidos falsos.
Robo de cuentas	Contraseñas repetidas, códigos compartidos o datos de recuperación desactualizados facilitan los accesos indebidos.
Redes y accesorios no confiables	Las redes wifi públicas o desconocidas y los cables o cargadores de origen dudoso aumentan la exposición.
Robo o pérdida	Un equipo sin bloqueo, cifrado ni localización deja expuesta la información guardada y las sesiones abiertas.

Cómo proteger tu dispositivo

- **Actualizá el sistema:** instalá las actualizaciones del sistema operativo y de las apps apenas estén disponibles; incluyen correcciones de seguridad.
- **Usá un bloqueo seguro:** configurá un PIN o contraseña robusta y un bloqueo automático en poco tiempo. La huella o el reconocimiento facial pueden sumarse como complemento.
- **Activá la autenticación multifactor:** sobre todo en el correo, las cuentas laborales, el banco y las redes sociales.
- **Instalá solo las apps que necesitás:** descargalas de tiendas oficiales y revisá quién las desarrolla, qué permisos piden, sus valoraciones y su última actualización.
- **Revisá los permisos:** limitá el acceso de cada app a la ubicación, la cámara, el micrófono, los contactos y los archivos según lo que realmente necesita.
- **Desconfiá de enlaces y archivos inesperados:** no abras adjuntos, códigos QR ni enlaces sin verificarlos, aunque parezcan venir de un contacto conocido.
- **Cuidá las conexiones:** apagá el Bluetooth, el wifi, el NFC y la ubicación cuando no los uses, y evitá operaciones sensibles en redes públicas.
- **Usá accesorios confiables:** evitá los puertos USB de carga públicos y usá tus propios cables y cargadores.

- **Hacé copias de seguridad:** respaldá tu información importante de forma periódica y comprobá que se pueda recuperar.
- **Preparate ante una pérdida o robo:** activá la localización, el bloqueo y el borrado remoto, y mantené al día los datos de recuperación de tus cuentas.

Privacidad y uso responsable

Ajustá la privacidad según el tipo de cuenta y lo que publicás. Revisá cada tanto quién puede ver tu información, qué apps tienen acceso a ella y con quién compartís tu ubicación. No alcanza con elegir una opción general como “Amigos”: también conviene revisar contactos, permisos y publicaciones anteriores.

En resumen

Actualizá	Instalá las correcciones del sistema y de las apps.
Protegé	Usá bloqueo seguro y autenticación multifactor.
Verificá	Revisá apps, permisos, enlaces y códigos QR antes de usarlos.
Respaldá	Hacé copias de seguridad y activá la localización o el borrado remoto.

La seguridad de tu celular depende de combinar actualizaciones, una buena configuración y hábitos responsables. Desde **BA-CSIRT** te acompañamos para que lo uses con más tranquilidad.