sedian

Seguridad Digital
de Andalucía

CONVIERTE TU DISPOSITIVO MÓVIL EN UNA CAJA FUERTE

¿Qué es **Android**?

Android es un sistema operativo basado en software de código abierto.

¿Qué **Ventajas** tiene Android?

- ✓ Su Personalización
- ✓ Múltiples dispositivos
- ✓ Es Asequible
- ✓ Su Código Abierto
- ✓ Totalmente Integrado con Google
- ✓ Libertad para el Usuario
- ✓ Multitarea

¿Por qué usar Android?

Algunas Ventajas del Sistema Operativo.

Primer Paso...

¿Cómo estás tratando a tu dispositivo?

Transforma tu teléfono en una “Caja fuerte”

Cuida tu dispositivo

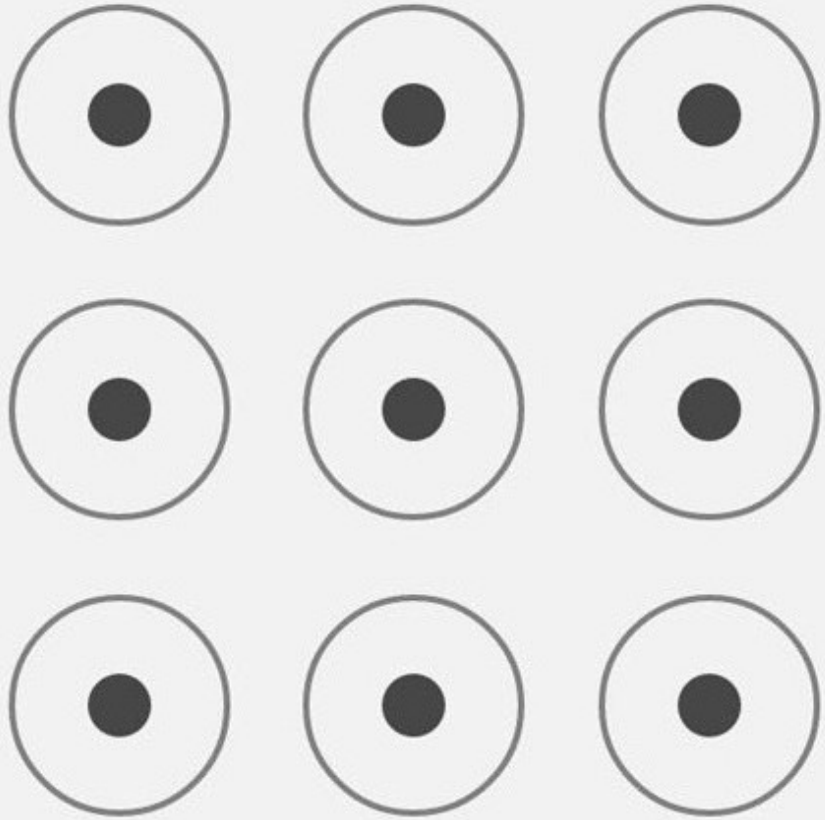
- **Nunca dejes un dispositivo desatendido en un lugar público. Si te lo roban o caen en otras manos podrán…**

- Hacerse pasar por ti en redes sociales
- Usar tu acceso al banco, compras, …
- Perder datos irremplazables
- Poner en peligro tu trabajo
- Llamar con tu número
- Suscribirte a servicios

Protege su Acceso

- **Si al salir de casa cierras las entradas, haz lo mismo con el móvil. ¿Cómo protegerte?**

- Revisa el manual del móvil para aprender todas las posibilidades de tu modelo.
- Distingue entre:
  - Controlar el acceso a tu móvil (el dispositivo)
  - Controlar el acceso a tu tarjeta sim



Protege su Acceso

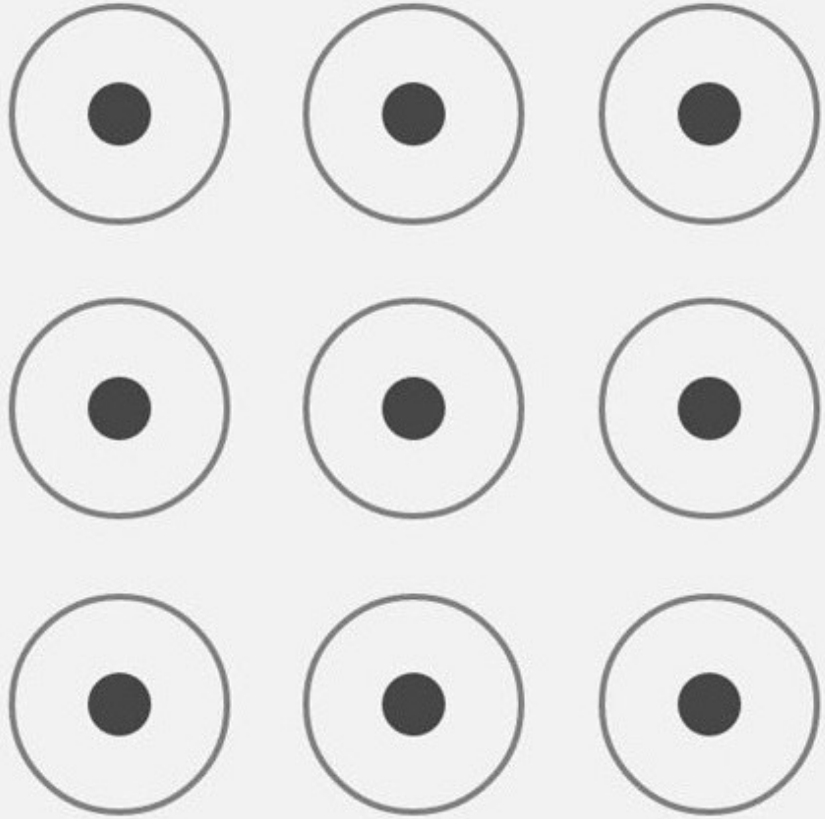
- **Si al salir de casa cierras las entradas, haz lo mismo con el móvil. ¿Cómo protegerte?**

- Para proteger nuestro dispositivo:

✓ Pon una contraseña que bloquee el arranque del dispositivo

✓ Pon siempre una contraseña o un patrón que bloquee el dispositivo de forma automática

✓ Nunca desactives la opción del PIN de la tarjeta sim



Protege su Acceso

- **Si no sabes donde está la opción que necesitas, usa el buscador.**

- Ve a la zona de ajustes y busca el lugar dedicado a la seguridad
- Según el modelo, lo encontrarás en :
  - Ajustes / Seguridad y Ubicación / Bloqueo de Pantalla
  - Ajustes / Pantalla Bloqueo

Protege su Acceso

- **Si no sabes donde está la opción que necesitas, usa el buscador.**

- Ve a la zona de ajustes y busca el lugar dedicado a la seguridad
- Según el modelo, lo encontrarás en :
  - Ajustes / Seguridad y Ubicación / Bloqueo de Pantalla
  - Ajustes / Pantalla Bloqueo
  - Busca los diferentes tipos de bloqueo de pantalla

Protege su Acceso

- **Si no sabes donde está la opción que necesitas, usa el buscador.**

- Ve a la zona de ajustes y busca el lugar dedicado a la seguridad
- Según el modelo, lo encontrarás en :
  - Ajustes / Seguridad y Ubicación / Bloqueo de Pantalla
  - Ajustes / Pantalla Bloqueo
  - Busca los diferentes tipos de bloqueo de pantalla
  - Selecciona el método mas adecuado para ti

Protege su Acceso

- **Si no sabes donde está la opción que necesitas, usa el buscador.**

- Ve a la zona de ajustes y busca el lugar dedicado a la seguridad
- Según el modelo, lo encontrarás en :
  - Ajustes / Seguridad y Ubicación / Bloqueo de Pantalla
  - Ajustes / Pantalla Bloqueo
  - Busca los diferentes tipos de bloqueo de pantalla
  - Selecciona el método mas adecuado para ti
    - Deslizar no añade seguridad

Protege su Acceso

- **Si no sabes donde está la opción que necesitas, usa el buscador.**

- Ve a la zona de ajustes y busca el lugar dedicado a la seguridad
- Según el modelo, lo encontrarás en :
  - Ajustes / Seguridad y Ubicación / Bloqueo de Pantalla
  - Ajustes / Pantalla Bloqueo
  - Busca los diferentes tipos de bloqueo de pantalla
  - Selecciona el método mas adecuado para ti
    - Deslizar no añade seguridad
    - Patrón nos pide dibujar un recorrido

Protege su Acceso

- **Si no sabes donde está la opción que necesitas, usa el buscador.**

- Ve a la zona de ajustes y busca el lugar dedicado a la seguridad
- Según el modelo, lo encontrarás en :
  - Ajustes / Seguridad y Ubicación / Bloqueo de Pantalla
  - Ajustes / Pantalla Bloqueo
  - Busca los diferentes tipos de bloqueo de pantalla
  - Selecciona el método mas adecuado para ti
    - Deslizar no añade seguridad
    - Patrón nos pide dibujar un recorrido
    - Pin y Contraseña nos dan una seguridad más alta

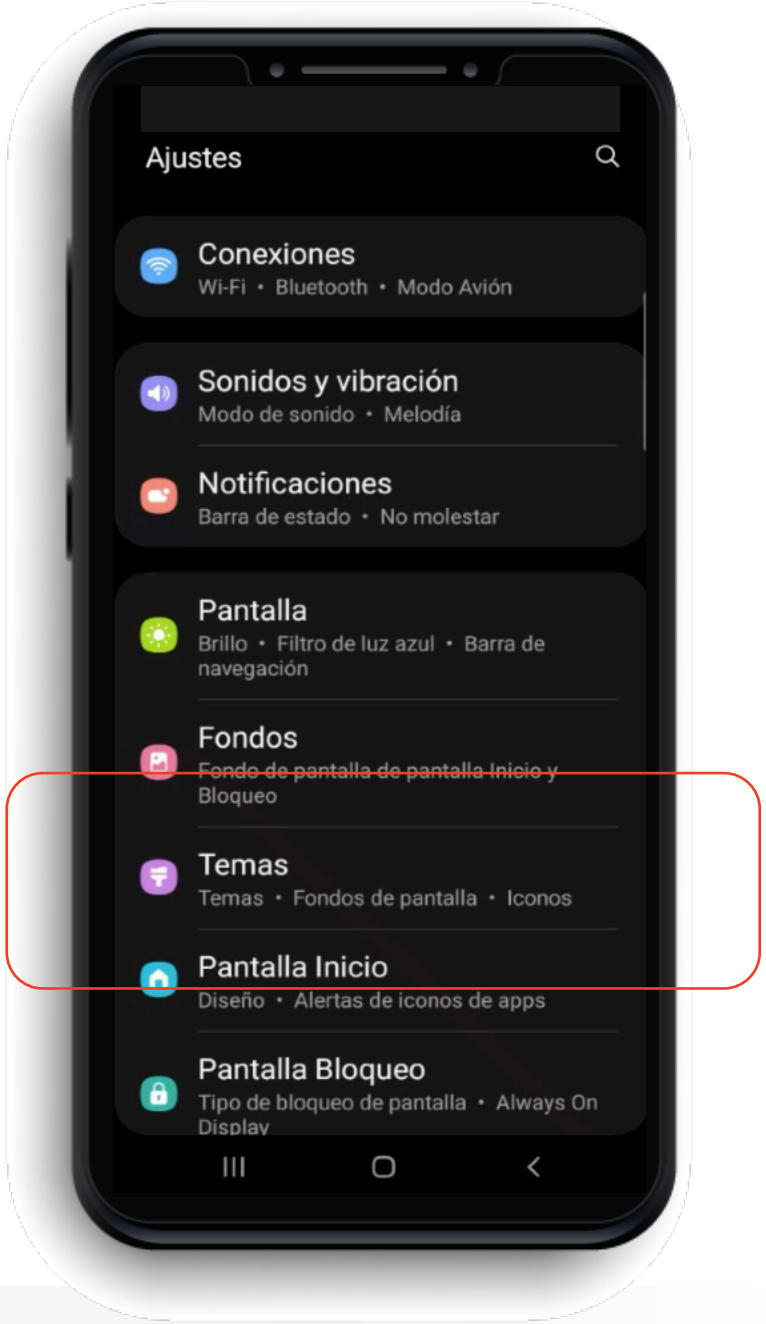
Protege su Acceso

- **Si no sabes donde está la opción que necesitas, usa el buscador.**

- Las opciones biométricas (reconocimiento del individuo por rasgos biológicos) son el mejor complemento para la seguridad

- Son elementos más avanzados que se encuentran en dispositivos de última generación

- Los más habituales son la huella dactilar y los patrones faciales.



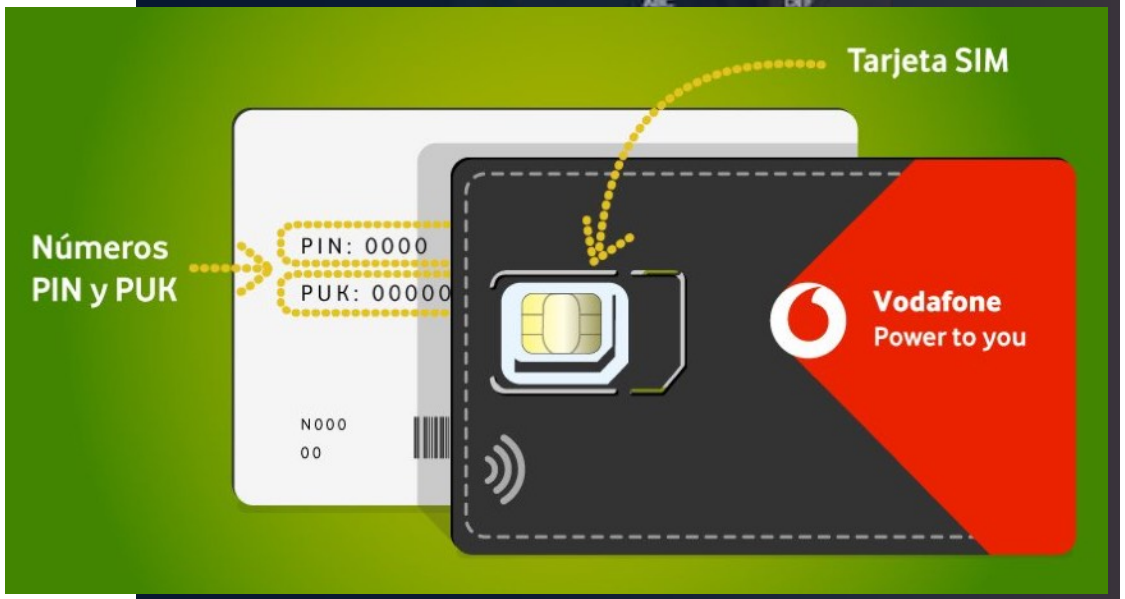
Protege su Acceso

- **Cuida tu PIN como si fuesen las llaves de tu casa.**

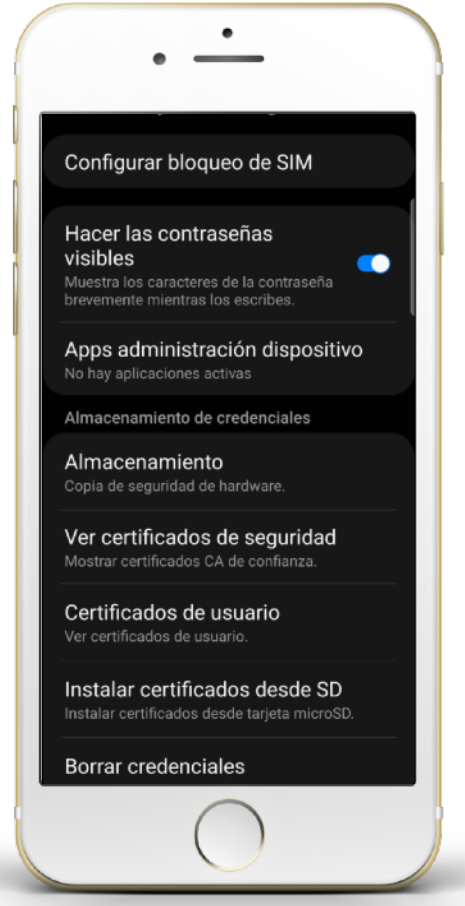
- ¿Qué son el **PIN** y el **PUK**?
- **PIN** : Número de 4 cifras para **activar** nuestra SIM

- ¿Qué sucede si olvido mi número PIN y se bloquea?
- **PUK**: Número de 8 dígitos para **recuperar** una SIM bloqueada

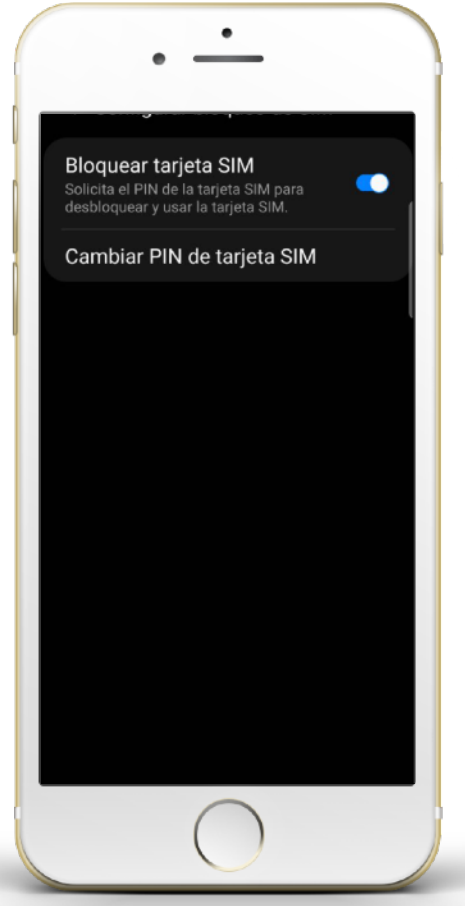
- ¿Dónde está mi **PUK**?



Configuración del PIN



Acceder a información del PIN



Cambiar la configuración

Cambiar el Pin

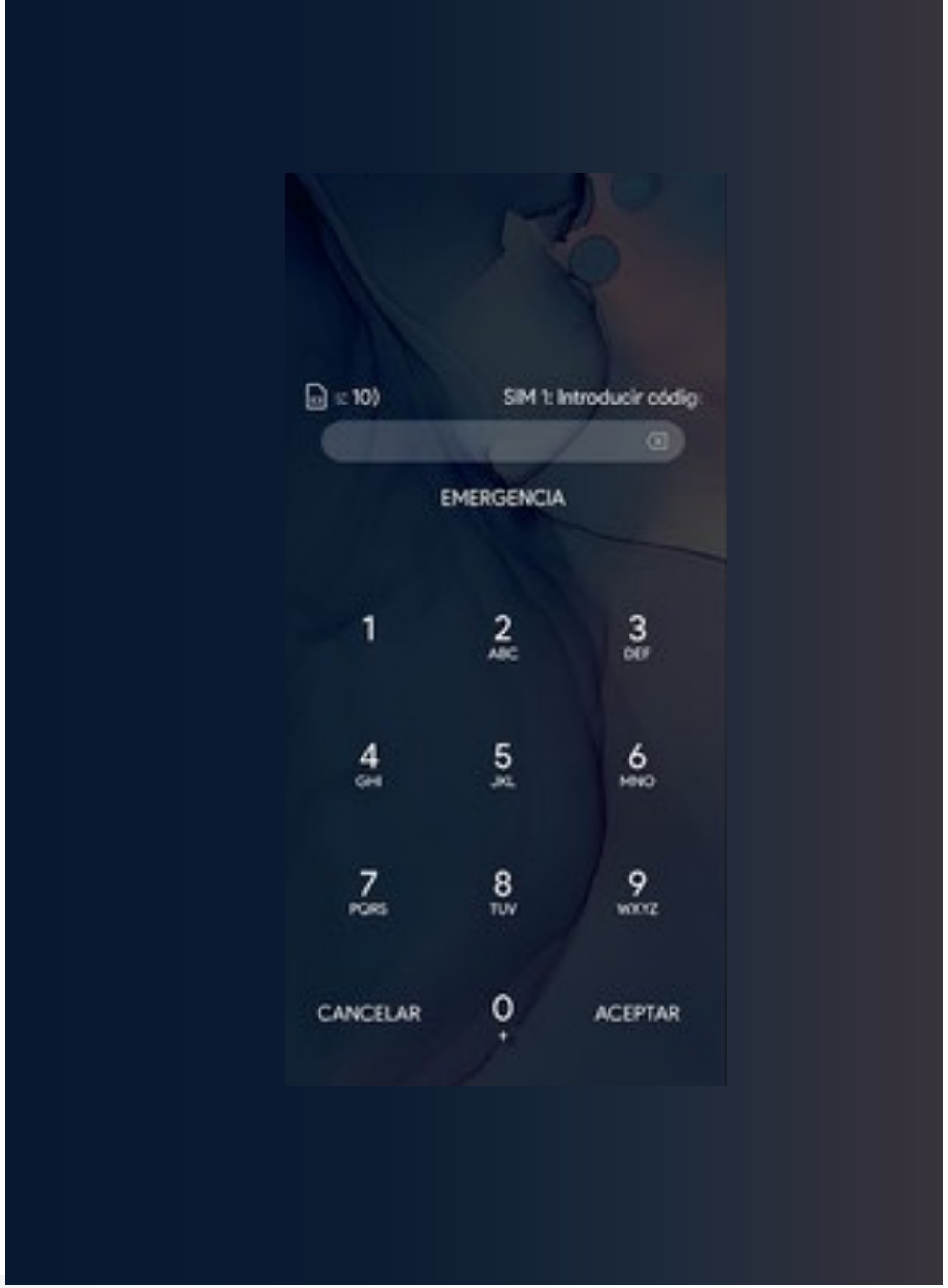
Protege su Acceso

- **Si pierdes tu móvil ¿Se puede bloquear a distancia?.**

- El **IMEI** es como el DNI de los teléfonos.

- Nuestra operadora sabe desde dónde se hace una llamada (SIM), y desde qué dispositivo (IMEI).

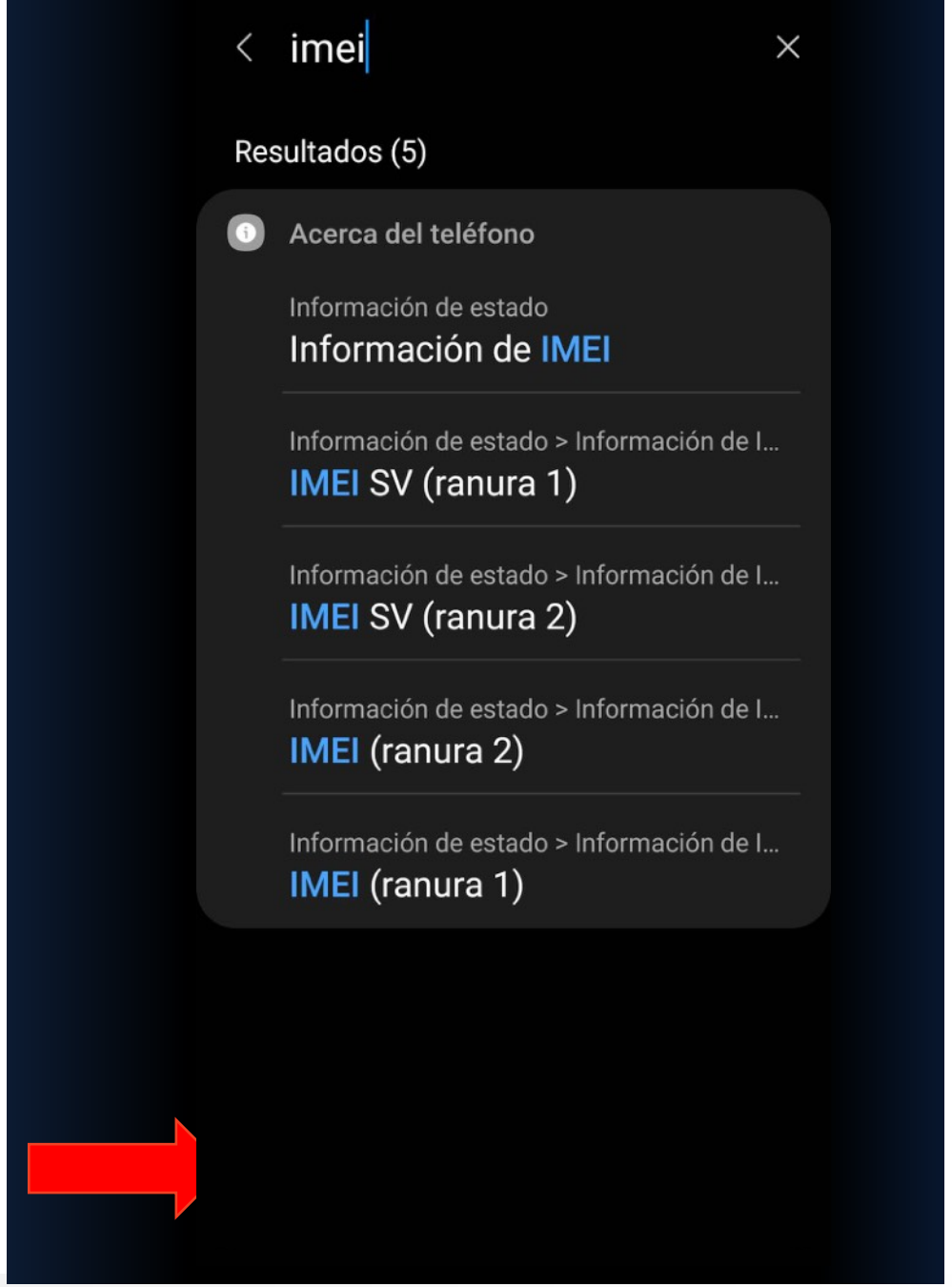
- El IMEI permite el bloqueo de terminales móviles en caso de robo, para lo cual simplemente tendremos que notificar el IMEI del móvil a nuestra operadora de telefonía para que proceda su bloqueo



Protege su Acceso

- **Si pierdes tu móvil ¿Se puede bloquear a distancia?.**

- ¿Dónde está el **IMEI**?
- Puede estar:
  - Impreso bajo la batería
  - En la caja del dispositivo
  - En una pegatina en la parte posterior del dispositivo. ¡CUIDADO!
  - Se puede consultar en los ajustes
  - Se puede marcar el código *#06# (asterisco, almohadilla, cero, seis, almohadilla) para que aparezca en la pantalla del dispositivo.



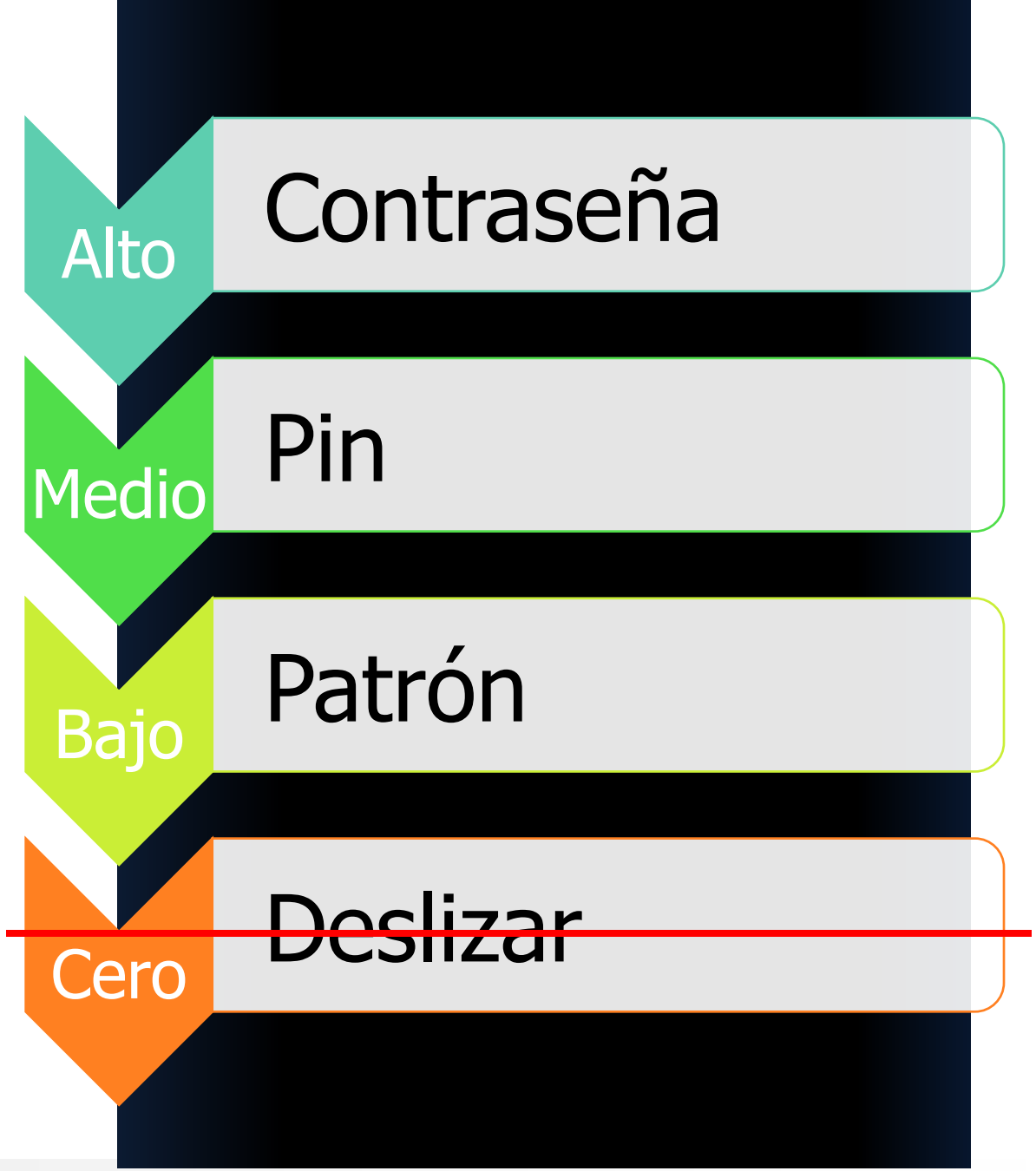
En resumen…

- **¿Qué debes hacer entonces?**

- Apunta el número de tu PIN, PUK e IMEI en un lugar seguro y que recuerdes. **NUNCA LO HAGAS** en el teléfono

- Elije un Método de bloqueo de Pantalla (o varios)

- Si tu modelo lo permite elige siempre al menos un método “Biométrico”



Jailbreaking o Rooting

La peligrosa liberación de tu dispositivo

¿Qué es?

Una Ruptura de los límites impuestos por el fabricante del dispositivo.

Nos convertimos en SuperUsuarios.

¿Para qué sirve?

Como superusuarios podemos manipular totalmente nuestro dispositivo.

Cambiar su S.O., eliminar aplicaciones predefinidas, instalar otras…

¿Es recomendable?

No. El fabricante no solo bloquea estas posibilidades por acciones comerciales, si no también por seguridad.

- ✓ Tus dispositivos son susceptibles a sufrir ataques
- ✓ Debes encargarte de su mantenimiento y actualizaciones
- ✓ Pierdes la garantía del dispositivo.

Segundo Paso...

El Riesgo de usar tu móvil

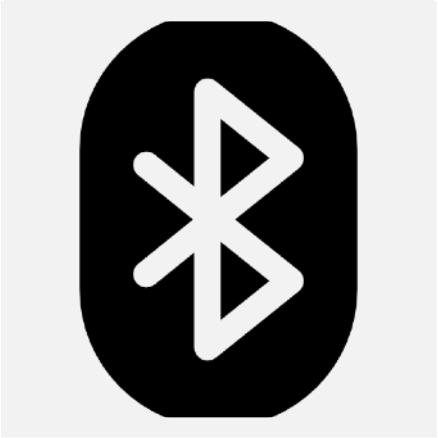
Conocer el peligro, la mejor arma para evitarlo.

Conexiones Activas

- **Dejar nuestro móvil abierto a conexiones que no estamos usando es una exposición innecesaria.**

WiFi

El **Wifi** permite la interconexión inalámbrica de dispositivos electrónicos.



Bluetooth

El **Bluetooth** posibilita la transmisión de voz y datos entre diferentes dispositivos mediante radiofrecuencia

NFC

NFC es una tecnología inalámbrica, que permite el intercambio de datos entre dispositivos cercanos.

GPS

GPS es un sistema que permite posicionar cualquier objeto sobre la Tierra de forma precisa.

Zona WiFi

Podemos crear una **Zona WiFi** que permite compartir nuestros datos con otros dispositivos.

Conexiones Activas

- **¿Qué problemas puede causar mantener estas conexiones activas?**
- Mediante un hackeo de canales bluetooth pueden **invadir tu privacidad** y, a partir de ahí, explotar otras violaciones de seguridad.
- Tener tu bluetooth activo en zonas masificadas **puede propiciar** esta situación. Apágalo.
- Un GPS activo puede **mostrar tu ubicación** de forma continuada y sin permiso incluso mediante aplicaciones que tú has instalado
- Crea una zona de compartición de wifi cifrada, siempre **con contraseña segura** y nunca aceptes un dispositivo que desconozcas
- No actives la comunicación NFS **hasta que vayas a usarla**, por ejemplo, para realizar un pago.
- Cambia los ajustes para que tu dispositivo **no se conecte** a un WIFI sin tu permiso y apágala si no la estas usando.

En resumen:





"Al igual que harías con el aire acondicionado, la vitrocerámica o el microondas; si no lo estás usando **APÁGALO**"

Tercer Paso...

De Cero a Héroe

Protegiendo tu información a capa y espada.

Evitar la trampa

Lo más importante para que alguien caiga en una trampa es un cebo bien jugoso.

Evitar la trampa

Lo más importante para que alguien caiga en una trampa es un cebo bien jugoso.

- **¿Cuál es el cebo?**
  - Al encontrar una red abierta podemos conectarnos sin problema.
  - Es muy atractiva en zonas abiertas como parques, estaciones o zonas comerciales, donde hay mayor cantidad de personas que están pasando el rato
  - También es habitual encontrar puestos de recarga de móviles mediante USB, ya que nos ayudan a recargar batería.

Red Wifi

Abierta

- **¿Cuál es la trampa?**
  - Al usar una red abierta cualquier persona puede conectarse a ella y ver los datos que enviamos (usuarios, contraseñas, pins, …).
  - También estamos expuestos al “Shoulder-Surfing” (el fisgoneo)
  - Los USBs no solo transmiten energía, también datos y “cualquier” extraño puede extraerlos desde el lugar donde los hemos conectado.

Evitar la trampa

Lo más importante para que alguien caiga en una trampa es un cebo bien jugoso.

- **¿Cómo evitar el peligro si necesitamos evitarlos?**
- Lleva a cabo [illegible] de bajo riesgo.
- No accedas a [illegible] relacionado con la banca online [illegible] (web o apps)
- Si vas a entrar en una [illegible] asegúrate de que sea segura (https con candado)
- Si entras en una web mediante usuario y contraseña, cierra sesión al finalizar
- Desactiva el envío de datos por USB
- Desactiva la sincronización.

+Alto	Banca online Paypal o Tarjetas de Crédito
Alto	Email y RRSS Trabajar documentos Online
Medio	Inicio de sesión en sitios
Bajo	Navegar Leer y Jugar

Evitar la trampa

El sentido común es el arma más importante para evitarlas

SPAM

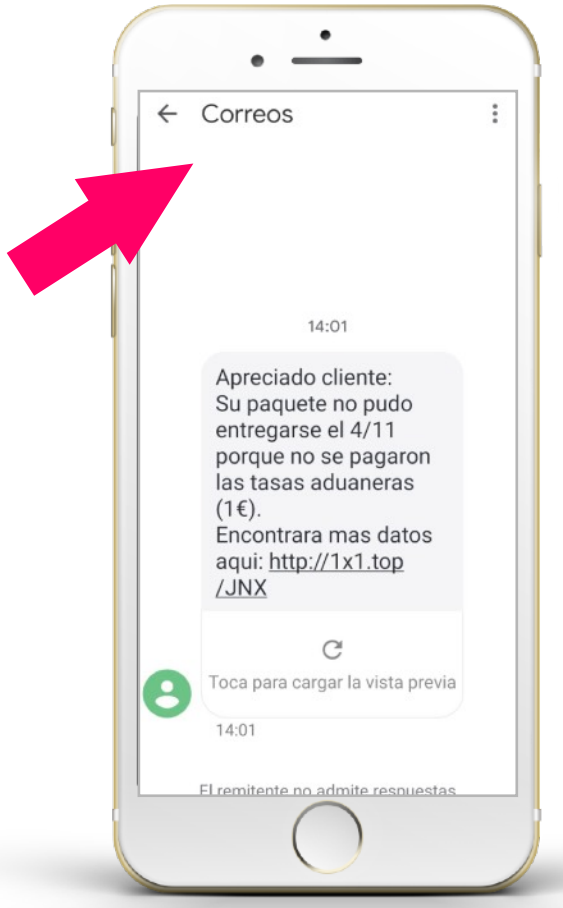
"Correo" no solicitado, no deseado o de remitente desconocido o falso

MALWARE

Programa malicioso destinado a realizar acciones dañinas en dispositivos electrónico

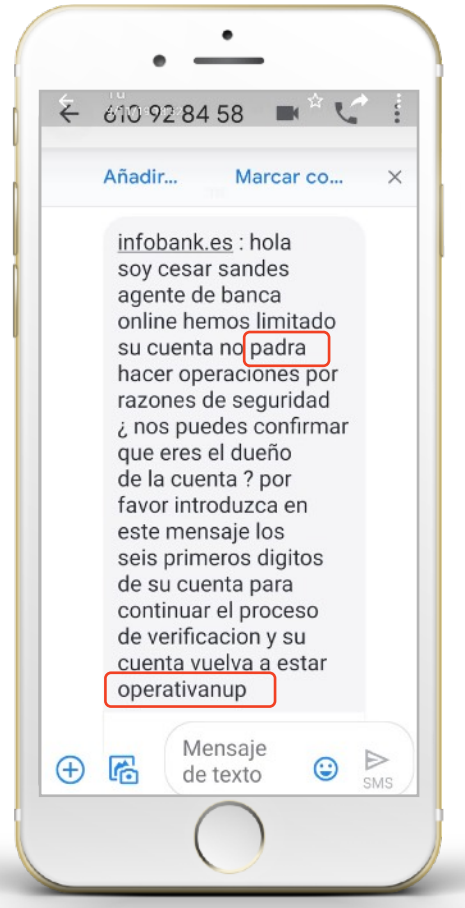
- ✓ No guardes nunca contraseñas o códigos PIN como un contacto
- ✓ No envíes ningún tipo de información, aunque parezca inofensiva, a desconocidos
- ✓ No hagas clic en ningún enlace o archivo desconocido
- ✓ No devuelvas llamadas a números desconocidos
- ✓ La banca no envía mensajes o códigos no solicitados

Ejemplos de Spam y Malware



Mensaje de Correos

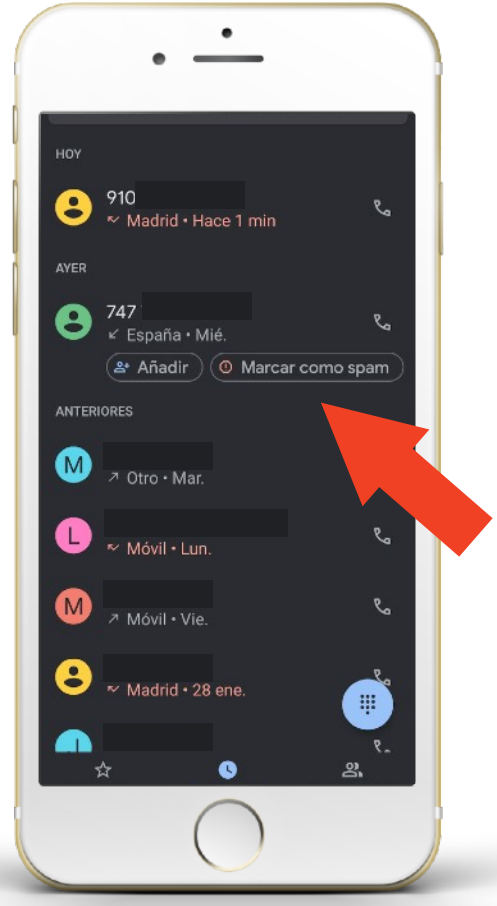
Mensaje de Caixa



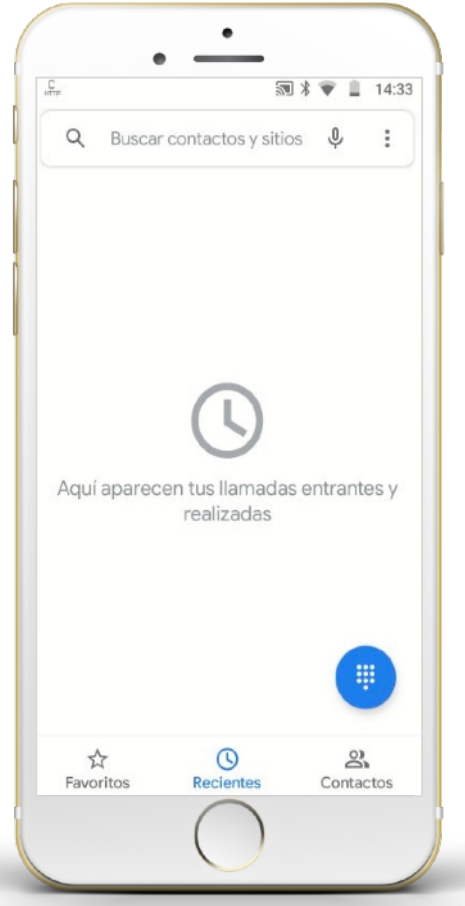
Mensaje de Infobank

Ejemplos de Spam y Malware

Detectada como Spam



Marcar como Spam

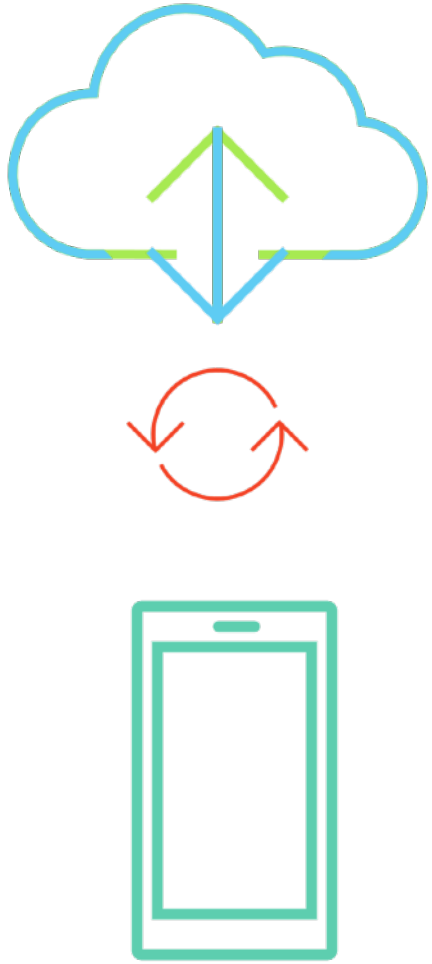


Protegerse del Spam

Copias de Seguridad

- **Tus datos siempre a salvo.**

- Las copias de seguridad nos sirven para mantener nuestros datos a salvo de posibles perdidas
- Al tener una cuenta de Google disponemos de un espacio en la nube llamada Drive donde podemos almacenar nuestros datos
- Una copia de seguridad nos permite recuperar nuestro “teléfono” incluso aunque lo perdamos o se haya estropeado



Copias de Seguridad

- **Activar nuestras copias**

- Las copias de seguridad no solo guardan nuestros datos de Google.
- También pueden guardar nuestras redes de wifi, sus contraseñas, nuestros contactos y datos de otras aplicaciones.
- Al iniciar un nuevo dispositivo solo tenemos que decirle que queremos restaurar estos datos y será como si no hubiésemos cambiado de móvil

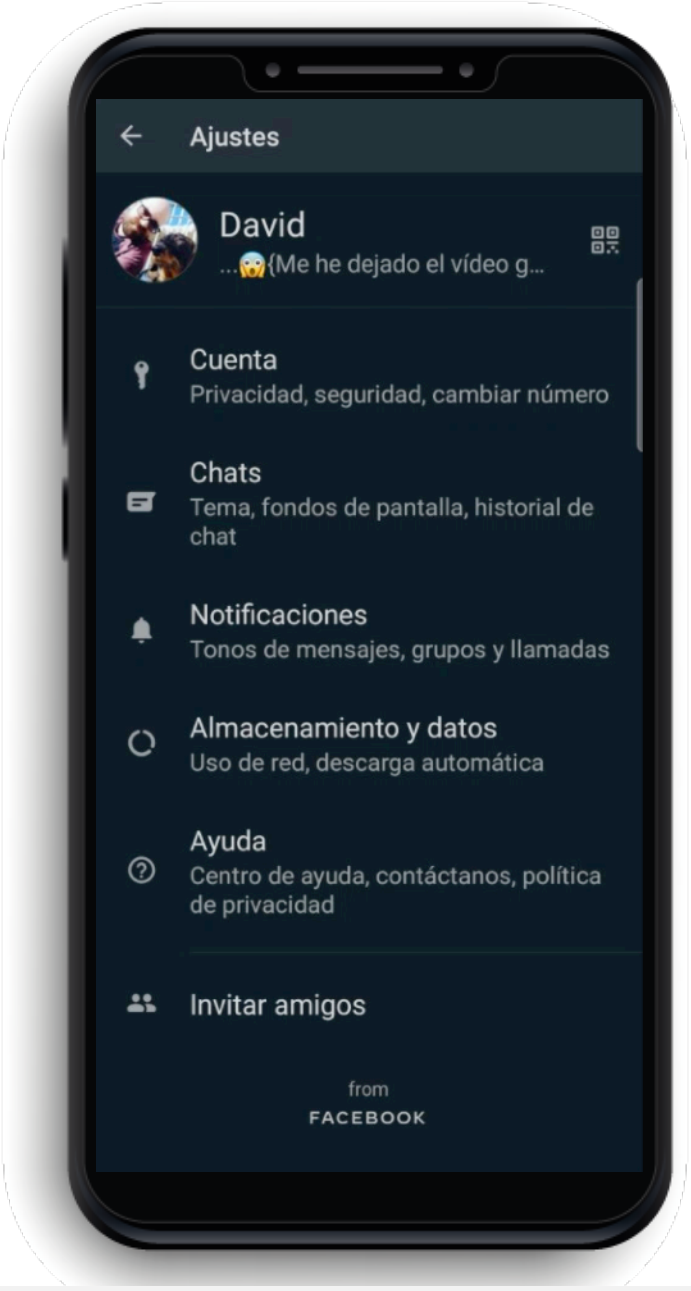
Copias de Seguridad

- **Activar nuestras copias**

- No solo Google hace copias de seguridad; también otras aplicaciones llevan a cabo este proceso.

- Una de las más usuales es WhatsApp, que nos da la posibilidad de realizar esta copia de seguridad también dentro de Google Drive

- Eso nos permitirá recuperar nuestros mensajes cuando iniciemos la aplicación en otro teléfono e incluso las fotografías y vídeos.



Último Paso...

Aplicaciones

Precauciones antes de usarlas.

Aplicaciones

Cuatro puntos que debes tener en cuenta antes de instalarlas y usarlas.

Oficiales

Descarga de tiendas oficiales

Investiga

Investiga puntuaciones y opiniones

Permisos

Revisa los permisos que debemos conceder

Actualiza

Manten sistema y aplicaciones actualizadas

Aplicaciones.

- **¿Son peligrosas las aplicaciones de nuestro dispositivo?**
- Muchas aplicaciones recogen y transmiten datos de tu dispositivo como información personal, ubicación, imágenes, contactos y mensajes.
- Sigue esto pasos para no tener problemas:

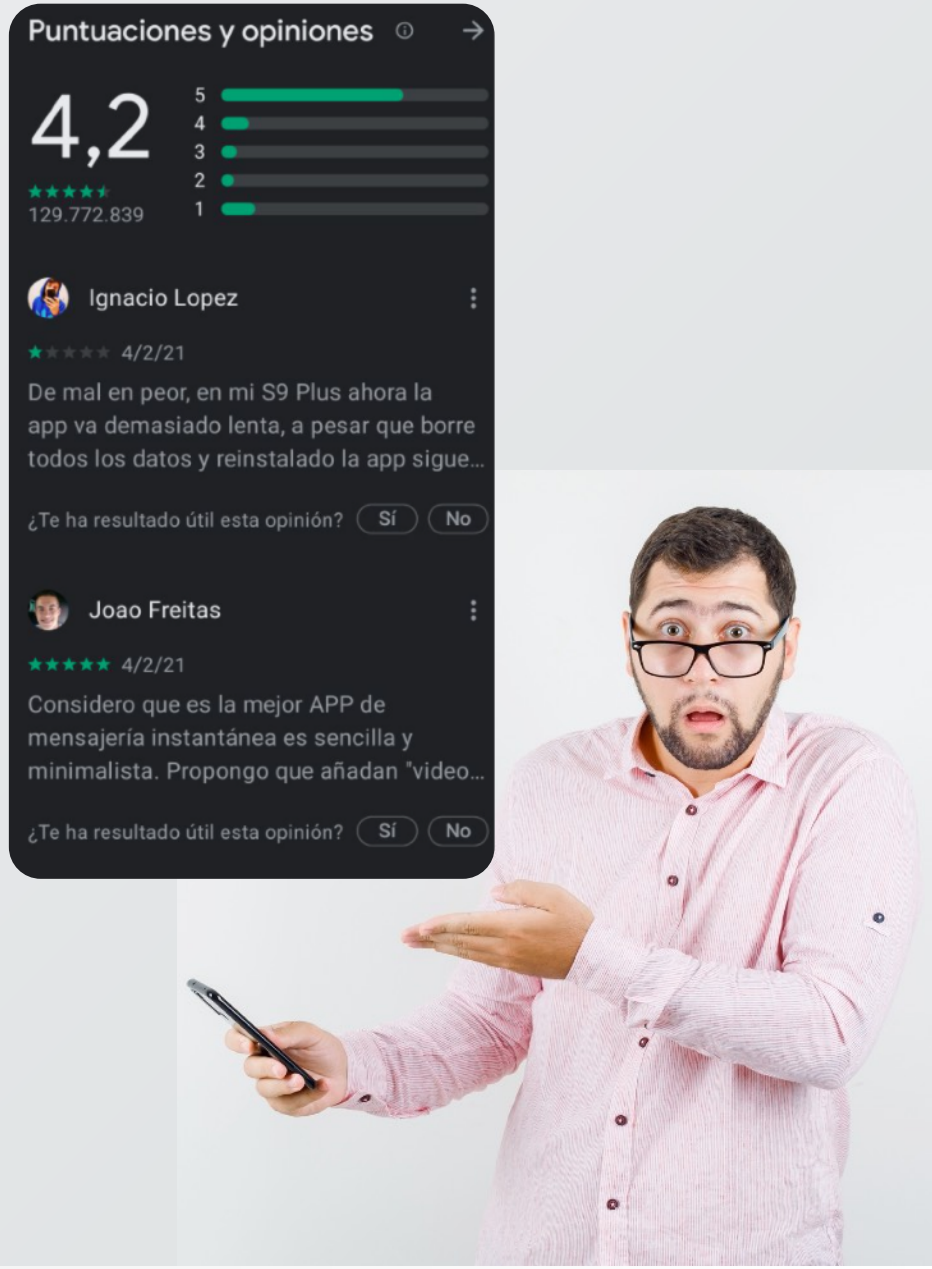
✓ Usa siempre la tienda oficial, Google Play Store

Aplicaciones.

- **¿Son peligrosas las aplicaciones de nuestro dispositivo?**
- Muchas aplicaciones recogen y transmiten datos de tu dispositivo como información personal, ubicación, imágenes, contactos y mensajes.
- Sigue esto pasos para no tener problemas:

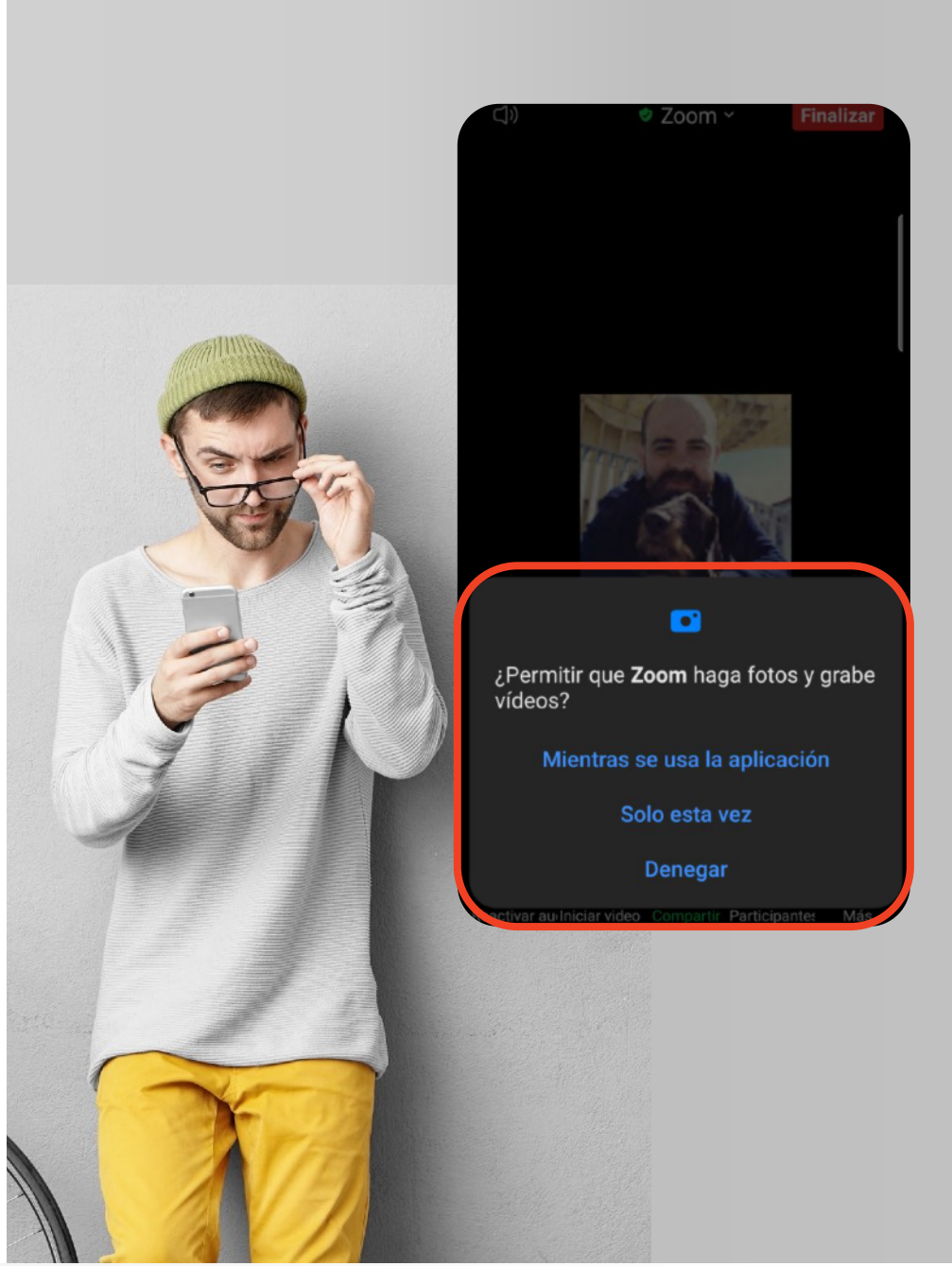
✓ Usa siempre la tienda oficial, Google Play Store

✓ Comprueba su puntuación y opiniones



Aplicaciones.

- **¿Son peligrosas las aplicaciones de nuestro dispositivo?**
- Muchas aplicaciones recogen y transmiten datos de tu dispositivo como información personal, ubicación, imágenes, contactos y mensajes.
- Sigue esto pasos para no tener problemas:



- ✓ Usa siempre la tienda oficial, Google Play Store
- ✓ Comprueba su puntuación y opiniones
- ✓ Observa los permisos de las aplicaciones. Si al instalarse te piden acceso a datos que consideras que no necesitan busca otra app similar.

Aplicaciones.

- **¿Son peligrosas las aplicaciones de nuestro dispositivo?**
- Muchas aplicaciones recogen y transmiten datos de tu dispositivo como información personal, ubicación, imágenes, contactos y mensajes.
- Sigue esto pasos para no tener problemas:

- ✓ Usa siempre la tienda oficial, Google Play Store
- ✓ Comprueba su puntuación y opiniones
- ✓ Observa los permisos de las aplicaciones. Si al instalarse te piden acceso a datos que consideras que no necesitan busca otra app similar.
- ✓ Mantén siempre actualizadas tus aplicaciones.

En resumen:

- ✓ Activa un **bloqueo de acceso** al dispositivo y de pantalla
- ✓ No dejes activas las conexiones que **no estés usando** en ese momento
- ✓ No te conectes a **redes abiertas**
- ✓ No aceptes archivos, enlaces o llamadas de **desconocidos**
- ✓ Instala solo **aplicaciones oficiales**.


sedian
Seguridad Digital
de Andalucía
Gracias
¡Y cuídate!