



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Taller “Seguridad en dispositivos: Android e iOS”



GOBIERNO DE ESPAÑA

VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL



TU AYUDA EN CIBERSEGURIDAD
incibe_



Oficina de Seguridad del Internauta



- ❖ 1. Bloqueo de pantalla.
- ❖ 2. Actualizaciones automáticas.
- ❖ 3. Software de seguridad.
- ❖ 4. Copias de seguridad.
- ❖ 5. Redes inalámbricas del dispositivo.
- ❖ 6. Descarga de aplicaciones desde un sitio seguro.
- ❖ 7. Permisos de aplicaciones.
- ❖ 8. Herramientas antirrobo.
- ❖ 9. Gestión de la memoria del dispositivo.
- ❖ 10. Guardando mis archivos en la nube de forma automática.
- ❖ 11. Rooting / Jailbreacking del dispositivo.
- ❖ 12. Cuestionario de evaluación

INTRODUCCIÓN

Nuestros dispositivos son una parte fundamental hoy en día.

Su uso abarca desde navegar por Internet a realizar compras online, por ello es tan importante que **conozcamos algunas de sus funciones de seguridad básicas, así como las tareas de mantenimiento o configuraciones de seguridad que podemos llevar a cabo junto a los procesos automáticos que las mejoran.**

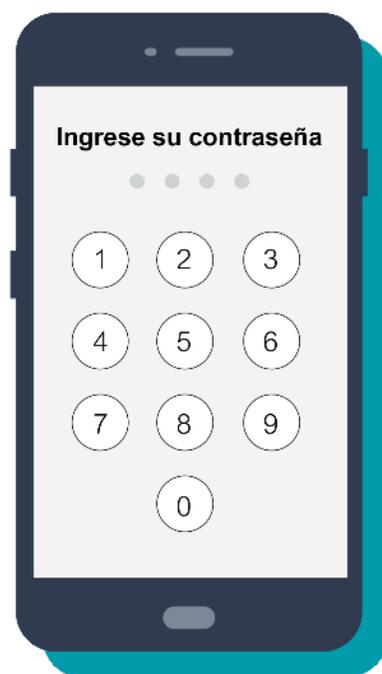


1. BLOQUEO DE PANTALLA

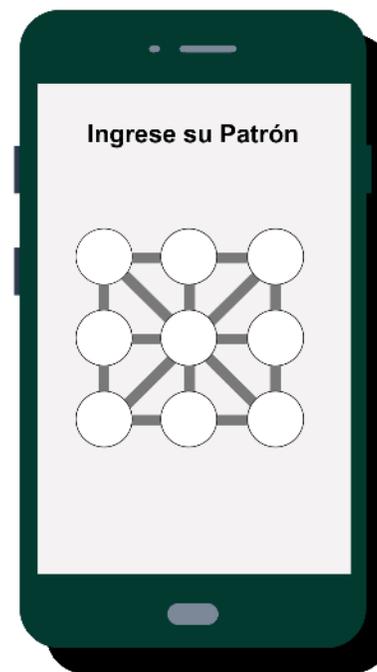
Bloquear nuestro dispositivo nos protege de **exponer nuestra información más desprotegida**. Por ello, es fundamental **configurar un bloqueo de pantalla**:



PIN



Contraseña



Patrón



Biometría



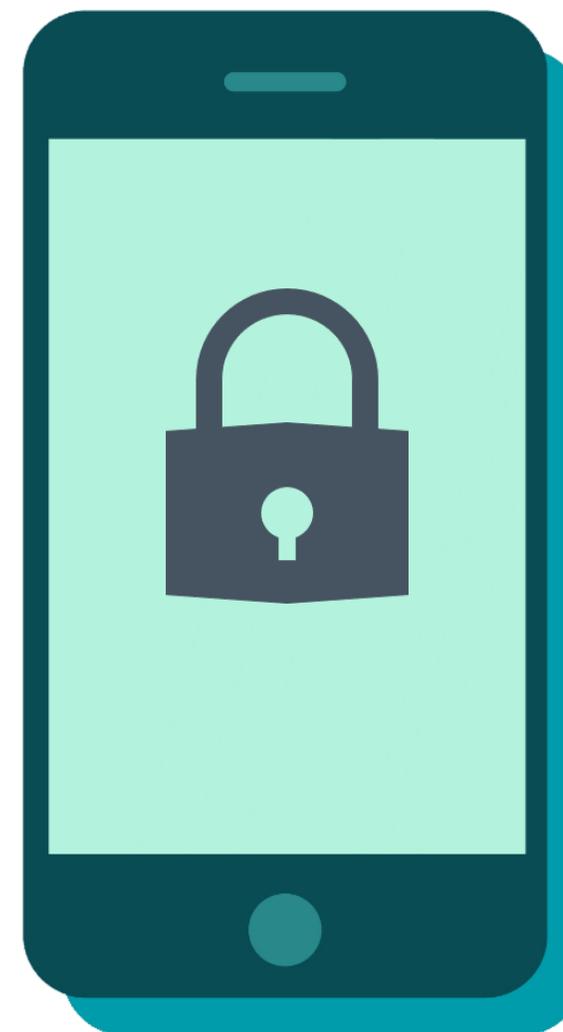
1. BLOQUEO DE PANTALLA

Para configurarlo en Android:

- ❖ Iremos **Ajustes > Seguridad > Bloqueo de pantalla.**

En iOS disponemos de varias funciones:

- ❖ **Bloquear con código de seguridad:** Ajustes > Touch ID y código.
- ❖ **Bloquear con Touch ID:** Ajustes > Touch ID > Agregar huella digital.
- ❖ **Bloquear con Face ID:** Ajustes > Face ID y código.
- ❖ **Bloqueo automático:** Ajustes > Pantalla y brillo > Bloqueo automático.



1. BLOQUEO DE PANTALLA: ACTIVIDAD



Configurar el bloqueo de pantalla es una de las primeras opciones que debemos realizar cuando nos hacemos con un dispositivo nuevo. Sin embargo, es probable que podamos mejorar la configuración para hacerla más segura. ¿Por qué no lo intentamos?

2. ACTUALIZACIONES AUTOMÁTICAS

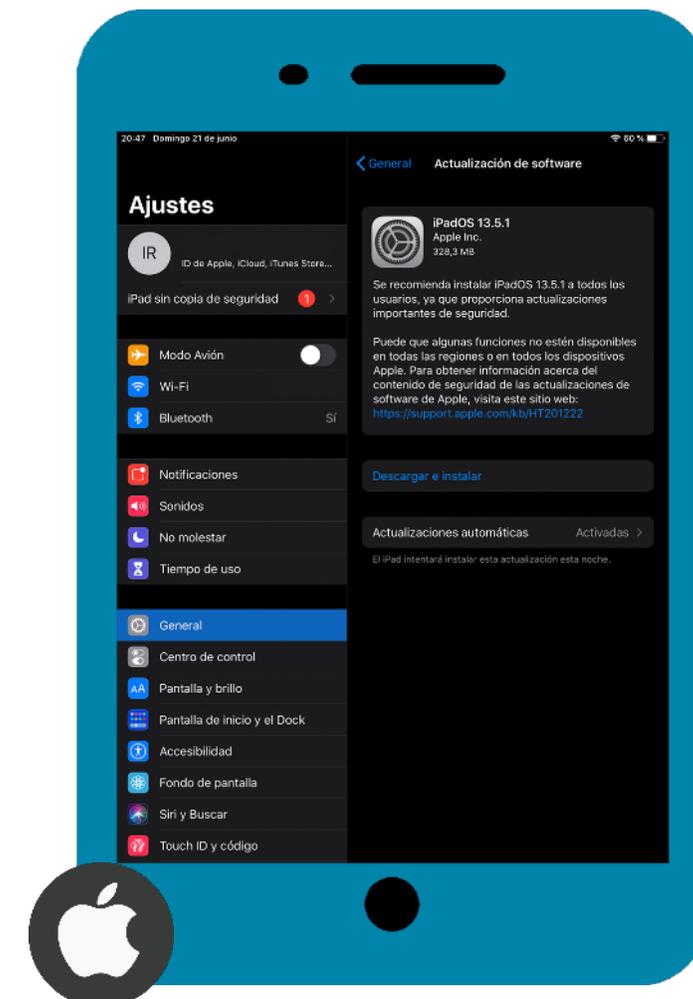
Las actualizaciones son fundamentales, ya que nos protegen de vulnerabilidades y errores o brechas en la seguridad de nuestro dispositivo.

Android:

- ❖ Accederemos a **Ajustes > Sistema > Ajustes avanzados > Actualización del sistema**. En otros modelos, será **Ajustes > Sobre el teléfono > Actualización del sistema**.

iOS:

- ❖ Iremos a **Ajustes > General y Actualización de software**.



2. ACTUALIZACIONES AUTOMÁTICAS

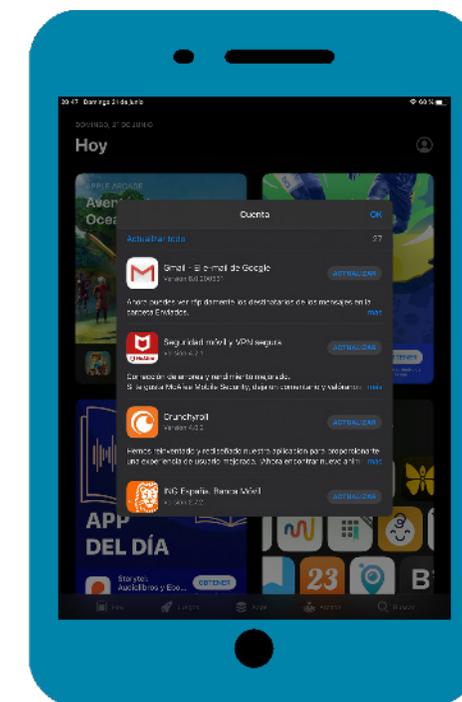
Es fundamental mantener actualizadas todas las **aplicaciones**:

Android:

- ❖ Ingresaremos en Google Play y descargarnos las últimas versiones o desde **Ajustes > Actualizar aplicaciones automáticamente** (o un nombre similar) y configurarlo.

iOS:

- ❖ Abriremos la **App Store > Hoy** y pulsaremos el icono de nuestro perfil para ver las actualizaciones pendientes, haciendo clic en **Actualizar** o **Actualizar todo**.
- ❖ Las actualizaciones automáticas pueden configurarse desde **Ajustes > ID Apple > iTunes Store y App Store** y activar la opción de **Actualizaciones de apps**.



2. ACTUALIZACIONES AUTOMÁTICAS: ACTIVIDAD



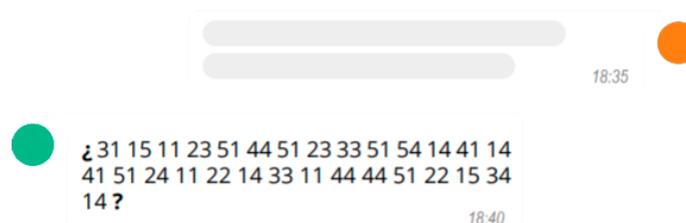
Un dispositivo actualizado está mejor preparado para defender nuestros datos de los ciberataques. Aunque pensemos que funciona perfectamente, nunca está de más asegurarnos de disponer de la última versión disponible, comprobándolo desde la configuración del dispositivo.

3. SOFTWARE DE SEGURIDAD

Existen miles de aplicaciones para los dispositivos móviles y, algunas de ellas, nos sirven para **mejorar la seguridad del dispositivo y nuestra privacidad**:



Aplicaciones de antivirus



Aplicaciones de cifrado



Bloqueo de aplicaciones



3. SOFTWARE DE SEGURIDAD



Gestores de contraseñas



Aplicaciones de verificación en dos pasos o factor múltiple de autenticación



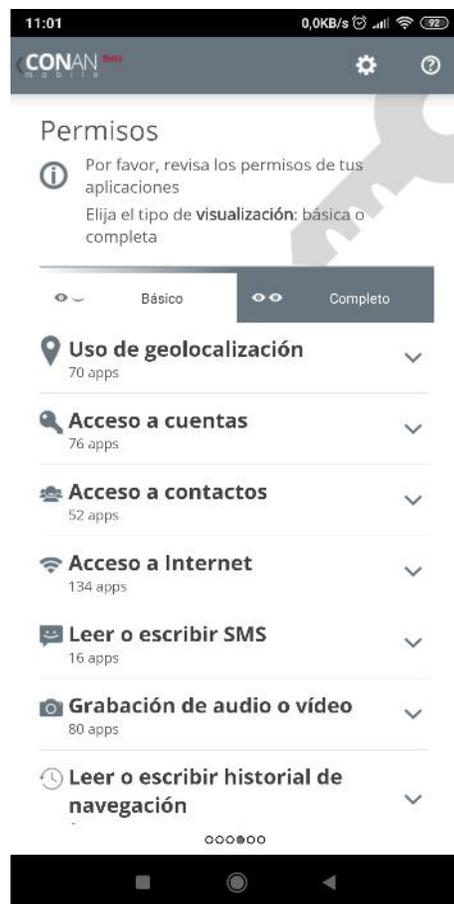
Aplicaciones de privacidad y navegación por Internet



3. SOFTWARE DE SEGURIDAD

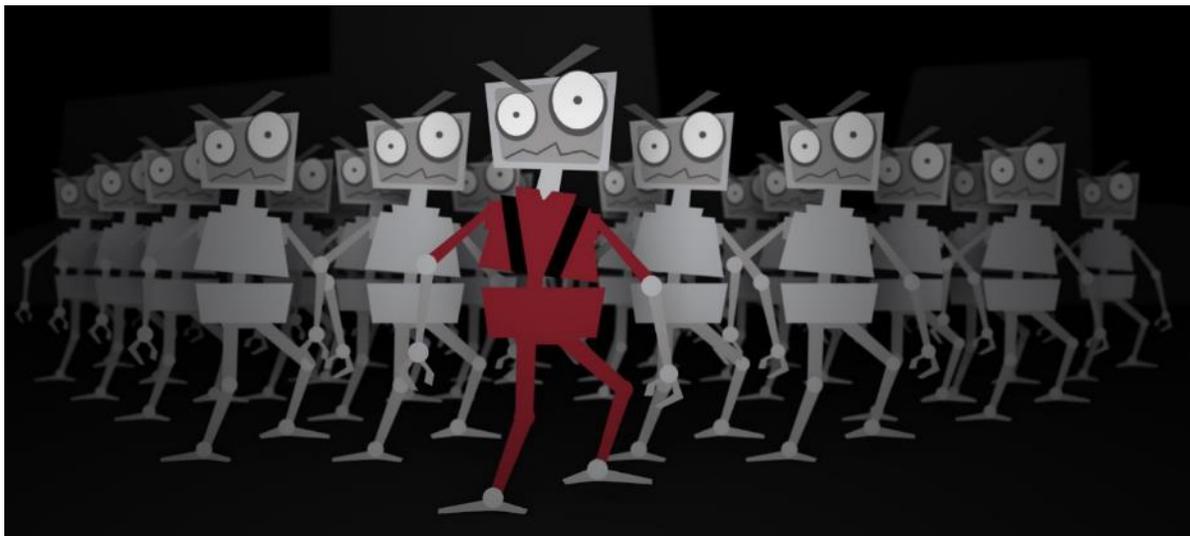


CONAN mobile es una aplicación para dispositivos Android, que ayuda a comprobar el nivel de seguridad de los dispositivos



3. SOFTWARE DE SEGURIDAD

El **Servicio Antibotnet** identifica si desde una conexión a Internet se ha detectado algún incidente de seguridad relacionado con botnets u otras amenazas.



Servicio
ANTIBOTNET

<https://www.osi.es/servicio-antibotnet>

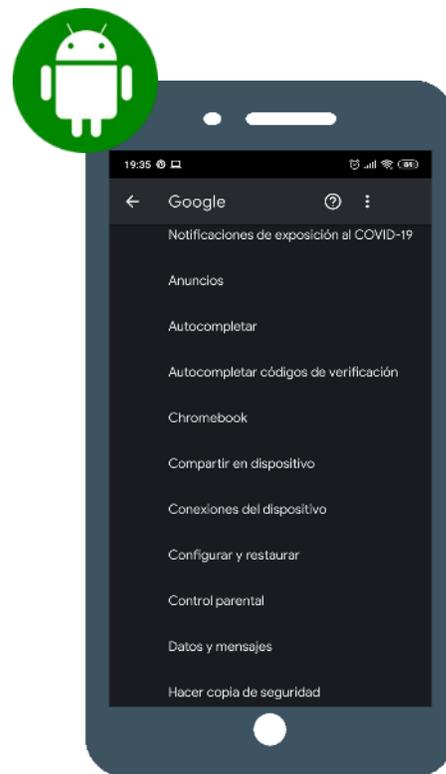
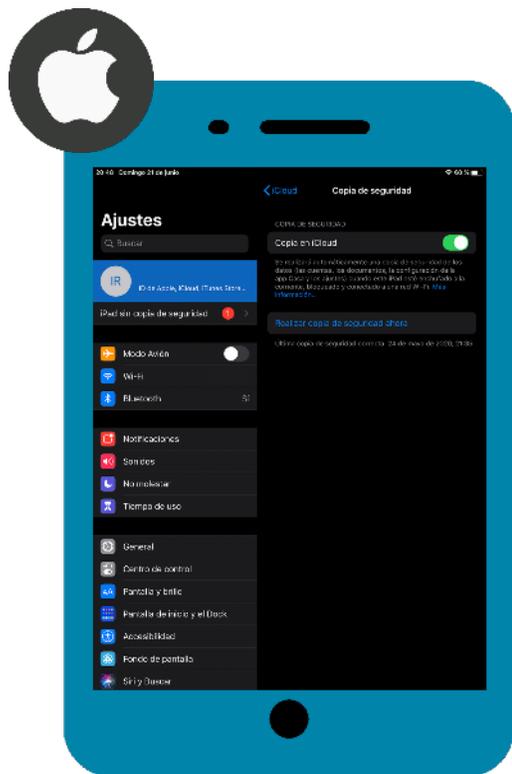


4. COPIAS DE SEGURIDAD

Las copias de seguridad permiten **mantener un doble de toda la información que tengamos almacenada en nuestro dispositivo.**



4. COPIAS DE SEGURIDAD



En Android:

❖ **Ajustes > Google > Hacer copia de seguridad.**

En iOS:

❖ **Ajustes > ID Apple > iCloud > Copia en iCloud.**

❖ **Para una copia manual Realizar copia de seguridad ahora.**



4. COPIAS DE SEGURIDAD: ACTIVIDAD



Configurar una copia de seguridad solo te llevará unos minutos y te dará la tranquilidad de disponer de una copia de tu dispositivo tal y como se encuentra en este momento. ¿A qué esperas?

5. REDES INALÁMBRICAS DEL DISPOSITIVO

Nuestros dispositivos inalámbricos tienen la posibilidad de conectarse a una gran variedad de redes inalámbricas.

Algunas sirven para tener **conexión a Internet**, **realizar pagos** con el mismo dispositivo o **conectarse a otros** para intercambiar archivos.



5.1 REDES INALÁMBRICAS DEL DISPOSITIVO: BLUETOOTH

El **Bluetooth** nos permite conectarnos a otro dispositivo para compartir archivos o emparejarlo con determinados dispositivos, como auriculares inalámbricos.



Tanto en **Android**, como en **iOS**, bastará con ir a **Ajustes > Bluetooth** para activar o desactivar esta función y acceder a su configuración.



5.2 REDES INALÁMBRICAS DEL DISPOSITIVO: WIFI

La red **wifi** nos permite navegar por Internet al conectarnos a una red wifi cercana a nuestro dispositivo.

- ❖ Una red abierta puede ser peligrosa., ya que corremos el riesgo de que alguien monitorice nuestra actividad.
- ❖ Es recomendable utilizar una VPN si es imprescindible conectarnos a una.
- ❖ Finalmente, no accedas a tus cuentas o servicios más personales.

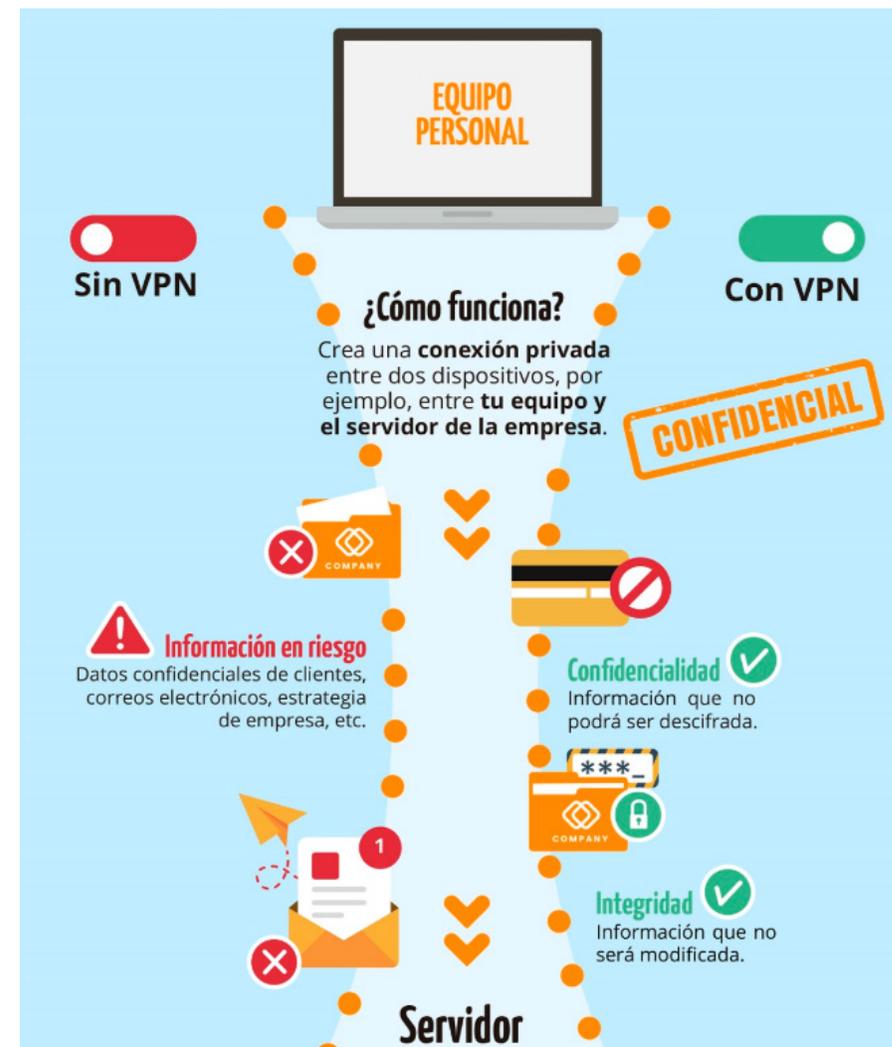


En **Android** e **iOS**, iremos a **Ajustes > Wi-Fi** para activar o desactivar esta función.



5.3 REDES INALÁMBRICAS DEL DISPOSITIVO: VPN

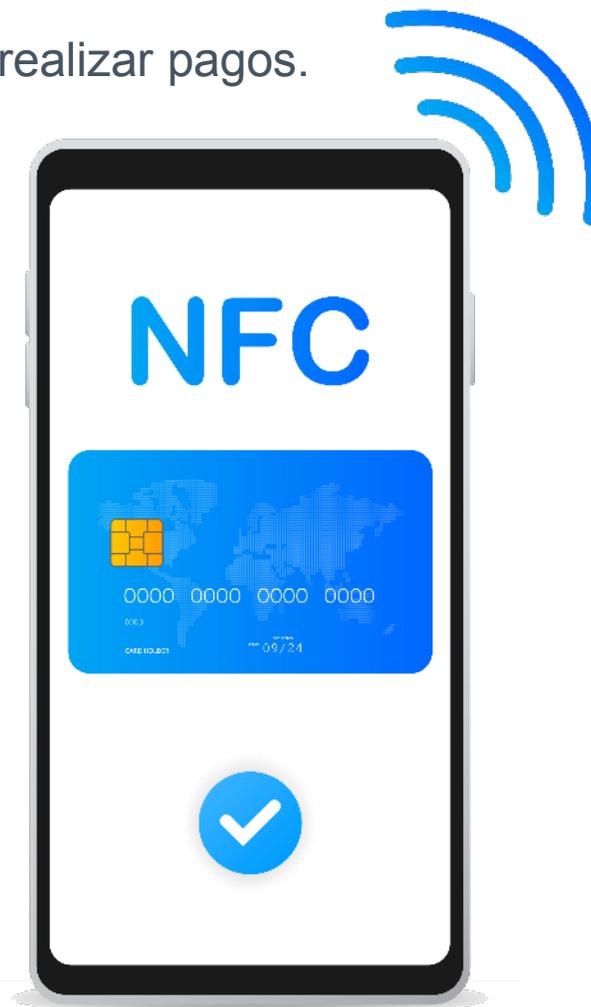
Las **Redes Privadas Virtuales o VPN** son un servicio que protege nuestra privacidad al cifrar la conexión entre nuestro dispositivo y el servidor VPN.



5.4 REDES INALÁMBRICAS DEL DISPOSITIVO: NFC

El **NFC** permite conectar dos dispositivos entre sí para intercambiar información, y realizar pagos.

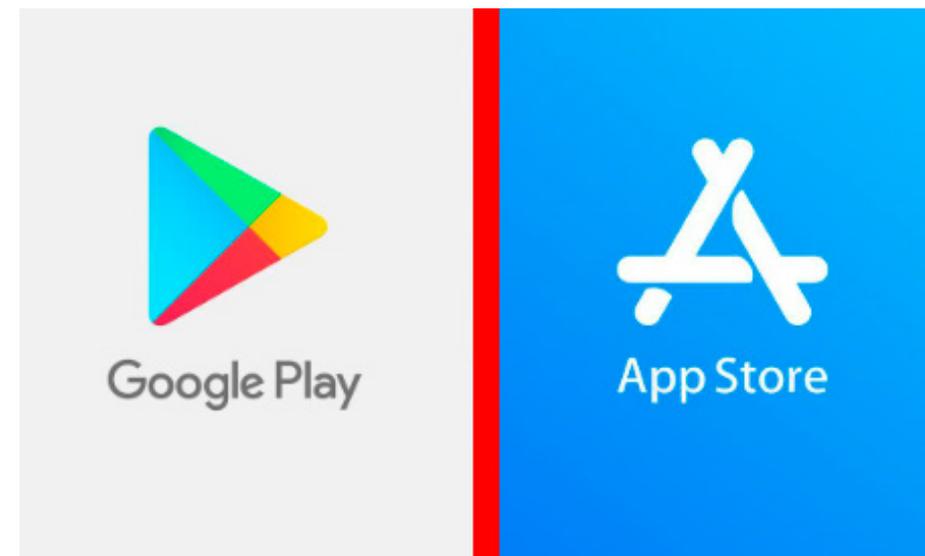
- ❖ **Android:** podemos activar o desactivar esta función desde **Ajustes > Conexiones > NFC**. Es necesario [Google Pay](#).
- ❖ **iOS:** esta función no puede activarse o desactivarse.



6. DESCARGA DE APLICACIONES DESDE UN SITIO SEGURO

Las aplicaciones son software que podemos instalar en nuestro dispositivo y que tienen muchísimas funcionalidades:

- ❖ Descarga solo de tiendas oficiales.
- ❖ Revisa quién es el desarrollador de la app.
- ❖ Echa un vistazo a los comentarios y valoraciones.
- ❖ Comprueba el número de descargas.



7. PERMISOS DE APLICACIONES

Cuando vamos a instalar una aplicación, esta nos pedirá una serie de permisos para funcionar. Una app maliciosa tratará de pedir todos los permisos posibles para poder actuar con libertad en nuestro dispositivo.

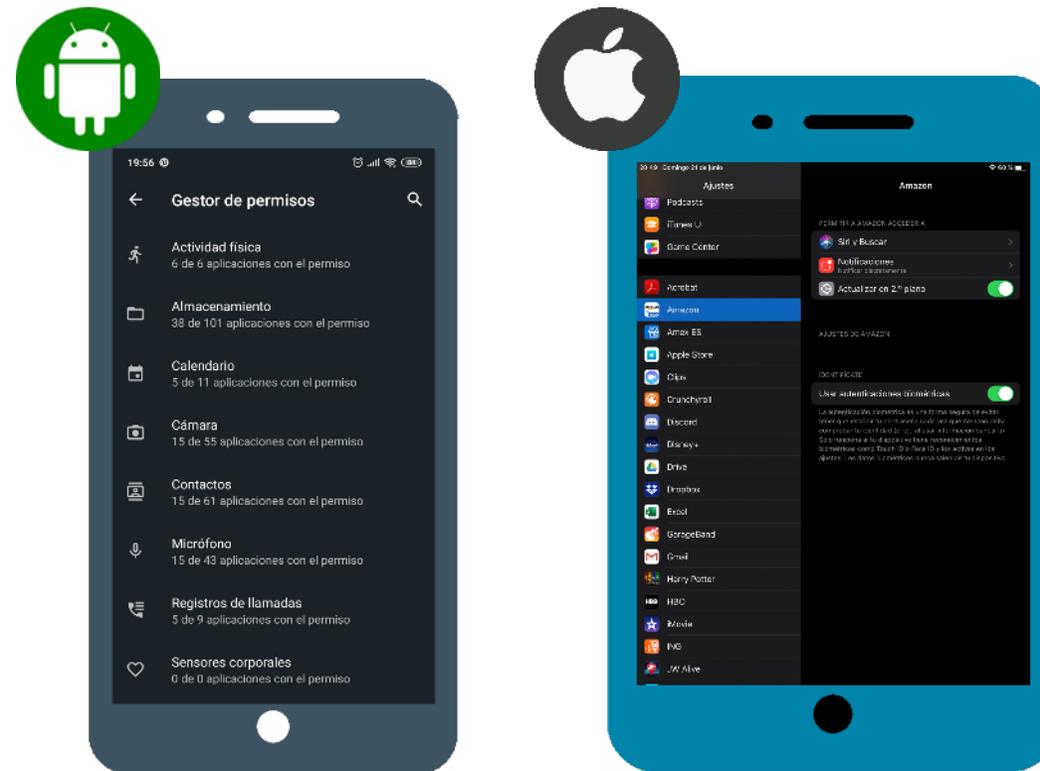
En **Android**:

❖ Iremos a **Ajustes > Aplicaciones > Permisos**.

Dentro, podremos ver una lista con todos los permisos que hemos concedido a las aplicaciones.

En **iOS**:

❖ Iremos a **Ajustes**. Y al final veremos las apps instaladas y sus permisos.



7. PERMISOS DE APLICACIONES



7. PERMISOS DE APLICACIONES: ACTIVIDAD



Seguro que tienes alguna aplicación instalada. Te invitamos a que accedas a tu dispositivo móvil y analices los permisos que diste a la última aplicación instalada. Prueba a revocar alguno si no lo ves necesario.

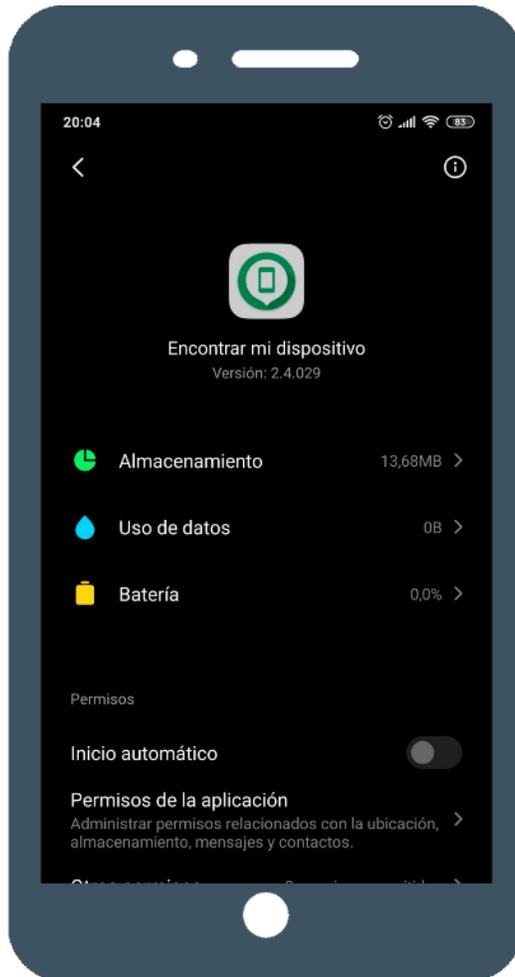
8. HERRAMIENTAS ANTIRROBO

Con la funcionalidad GPS activada muchas aplicaciones pueden recopilar y compartir nuestra ubicación y, aunque en ocasiones pueda suponer un **riesgo para nuestra privacidad**, si la utilizamos con cabeza, también puede ayudarnos.

Aquí entran las **herramientas antirrobo** que actúan rápidamente en caso de pérdida o robo de nuestro dispositivo.



8.1 HERRAMIENTAS ANTIRROBO ANDROID

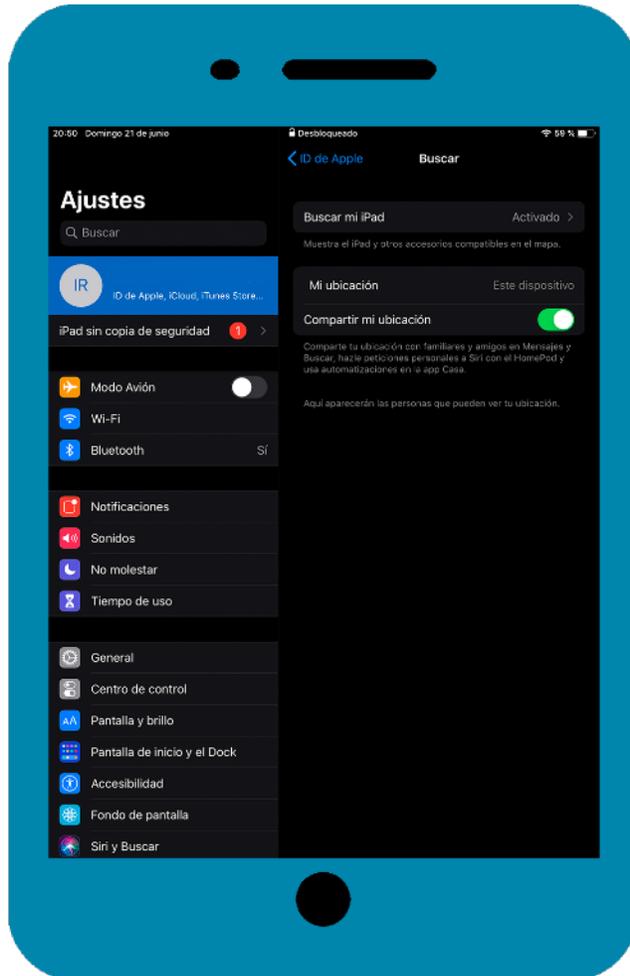


En el caso de **Android**, disponemos de la opción **Administrador de dispositivos**.

- ❖ Iremos a **Ajustes > Estado de seguridad / Seguridad y ubicación o Google > Seguridad**.
- ❖ Nos aseguraremos de que la función [Encontrar dispositivo](#) esté activada y actualizada.
- ❖ Podemos comprobar que la herramienta funciona desde: <https://android.com/find>.



8.2 HERRAMIENTAS ANTIRROBO iOS



Con **iOS** podemos utilizar la función **Buscar mi iPhone/iPad**.

- ❖ Iremos a **Ajustes > Privacidad > Localización** para activarla.
- ❖ Activaremos **Permitir localización sin conexión**. Y, si queda poca batería, activaremos **Enviar última ubicación**.
- ❖ Luego, **Ajustes > [nombre] > Buscar** para activar la opción **Buscar mi iPhone/iPad**.
- ❖ Podemos probar esta función ingresando con nuestra cuenta de Apple en: <https://www.icloud.com/find>.

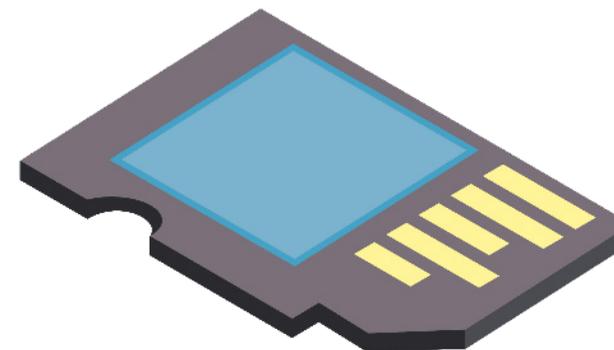


9. GESTIÓN DE LA MEMORIA DEL DISPOSITIVO

Nuestro dispositivo tiene una memoria limitada que se va llenando a medida que instalamos aplicaciones y guardamos información.



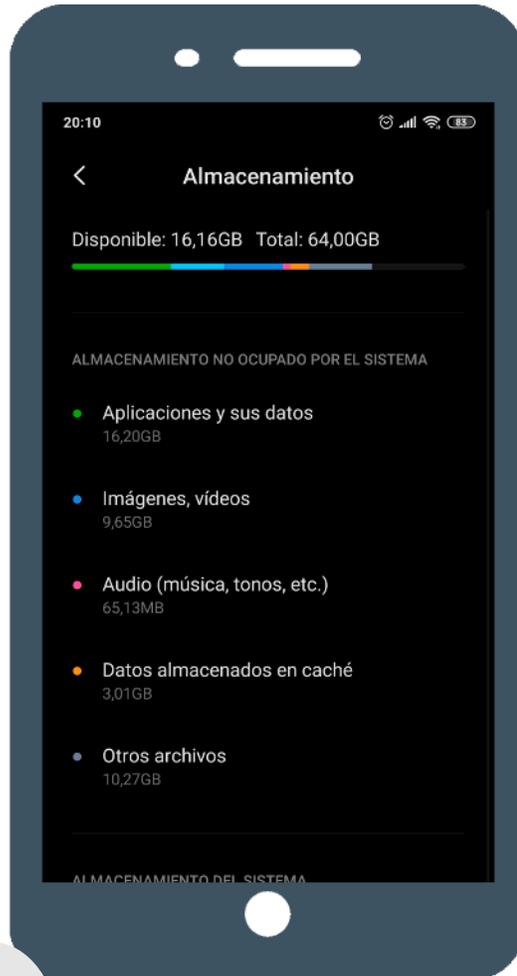
Memoria interna



Memoria externa



9.1 GESTIÓN DE LA MEMORIA DEL DISPOSITIVO ANDROID



En el caso de **Android**, iremos a **Ajustes > Sobre el teléfono > Almacenamiento**.

Si queremos **liberar espacio de apps y datos**:

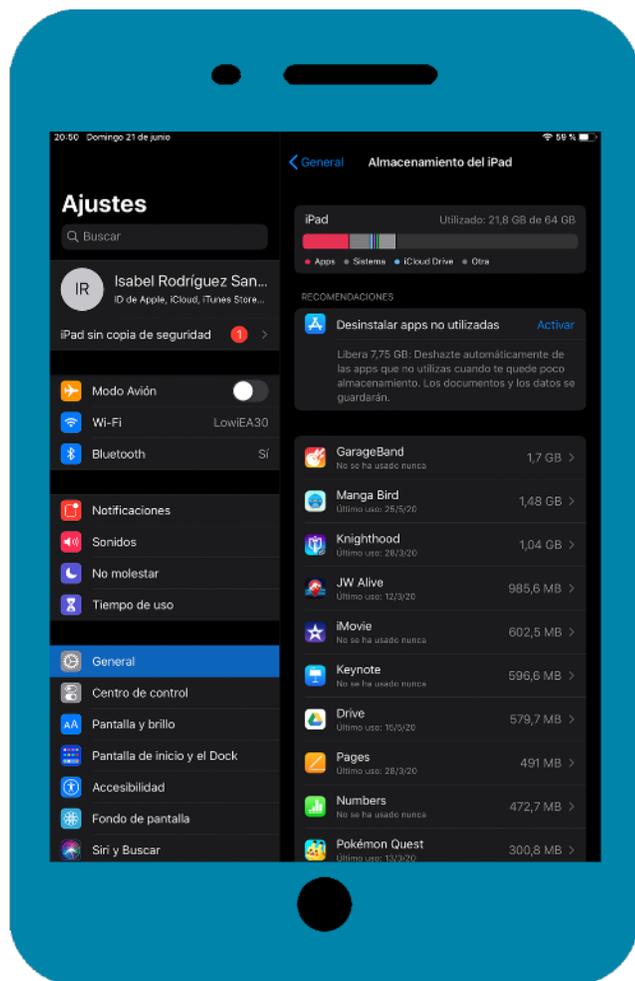
- ❖ Iremos a **Ajustes > Aplicaciones > Administrar aplicaciones**.
- ❖ Luego, podremos **Borrar caché o Borrar datos**.

Si queremos **liberar espacio de archivos**:

- ❖ Iremos a **Archivos o Gestor de archivos** y eliminaremos lo que queramos.



9.2 GESTIÓN DE LA MEMORIA DEL DISPOSITIVO iOS



En el caso de **iOS**, podemos consultar el almacenamiento desde **Ajustes > General > Almacenamiento del dispositivo**. Dentro, dispondremos de algunas recomendaciones para liberar espacio, como **Desinstalar apps no utilizadas**.

- ❖ **Desinstalar app.**
- ❖ **Eliminar app.**



9.3 GESTIÓN DE LA MEMORIA DEL DISPOSITIVO: ACTIVIDAD

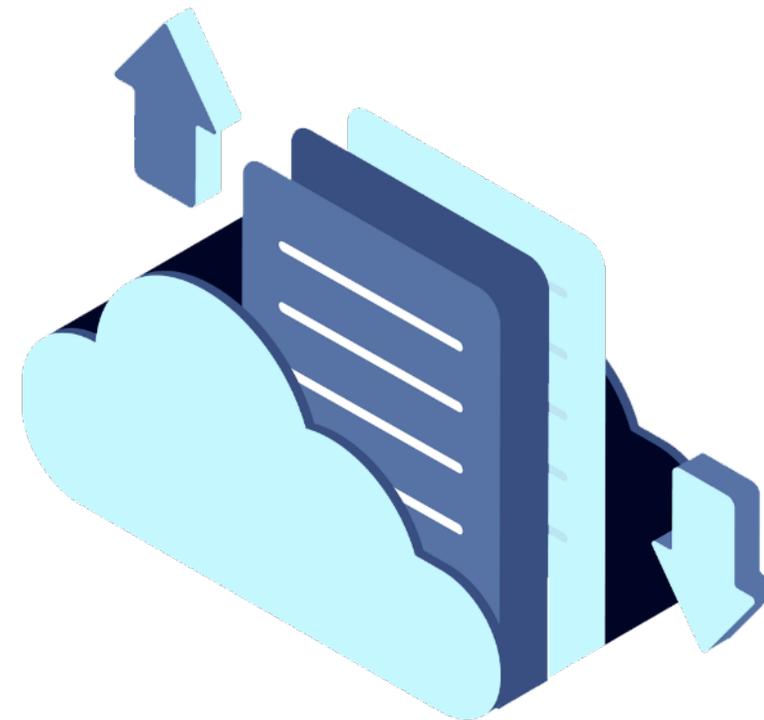


Si descuidamos la memoria de nuestro dispositivo, puede que acabemos quedándonos sin espacio muy pronto. Ya sean fotografías vídeos o apps que no utilizas, una limpieza a tiempo te ayudará en el futuro. Accede a la configuración y haz una limpieza ligera para disponer de espacio suficiente para futuras actualizaciones de seguridad, por ejemplo.

10. GUARDANDO MIS ARCHIVOS EN LA NUBE DE FORMA AUTOMÁTICA

La nube nos permite disponer de un servicio de almacenamiento en la Red para no tener que estar constantemente eliminando u organizando la información de nuestro dispositivo.

Además, nos permite disponer de un lugar donde almacenar nuestras copias de seguridad.



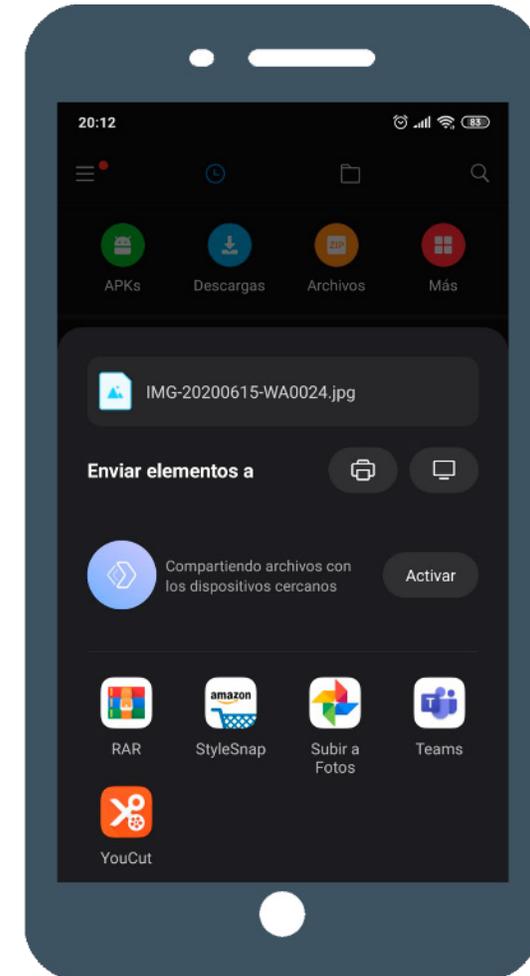
10.1 GUARDANDO MIS ARCHIVOS EN LA NUBE DE FORMA AUTOMÁTICA ANDROID

En **Android**, gracias a nuestra cuenta de Google tendremos acceso al almacenamiento en la nube de **Google Drive** y **Google Fotos**.

Podemos configurarlo a nuestro gusto en **Ajustes > Cuenta y sincronización / Cuentas > Google**

Para hacerlo de forma manual:

- ❖ Iremos a **Ajustes / Gestor de archivos** y **Enviar**.
- ❖ Luego, seleccionaremos un servicio u otro..



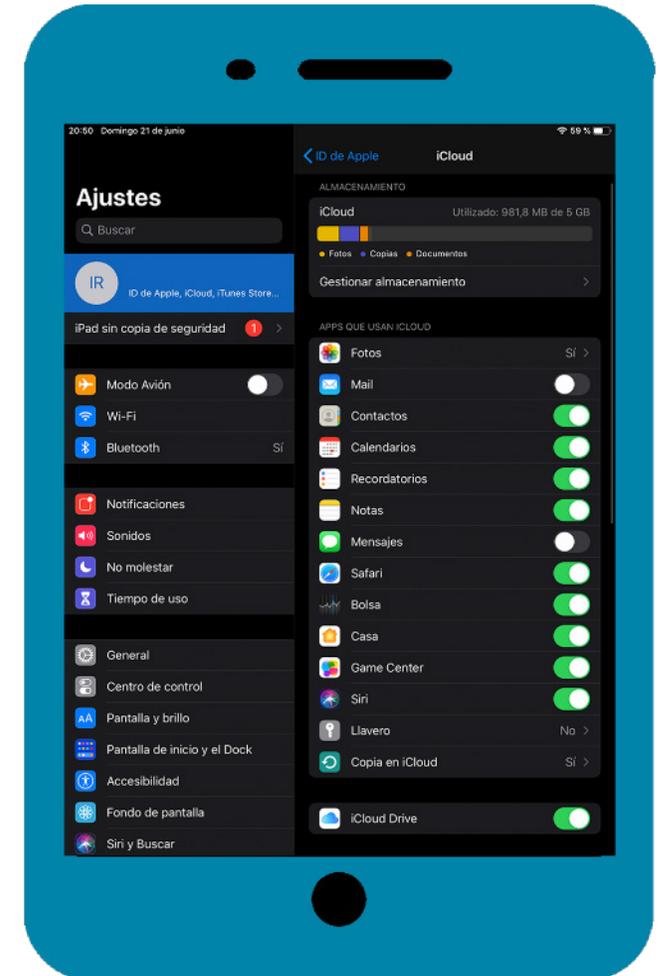
10.2 GUARDANDO MIS ARCHIVOS EN LA NUBE DE FORMA AUTOMÁTICA iOS

En **iOS** también hay disponible un servicio en la nube conocido como **iCloud**.

Para subir archivos a la nube:

❖ Iremos a **Configuración > ID Apple > iCloud Drive**.

Para gestionar nuestros archivos de iCloud Drive necesitaremos la [app Archivos](#).



11. ROOTING / JAILBREAKING DEL DISPOSITIVO

Estos términos hacen referencia a procedimientos mediante los cuales pueden 'liberarse' los dispositivos móviles, **eliminando las restricciones de los fabricantes:**



Rooting (Android)



Jailbreaking (iOS)

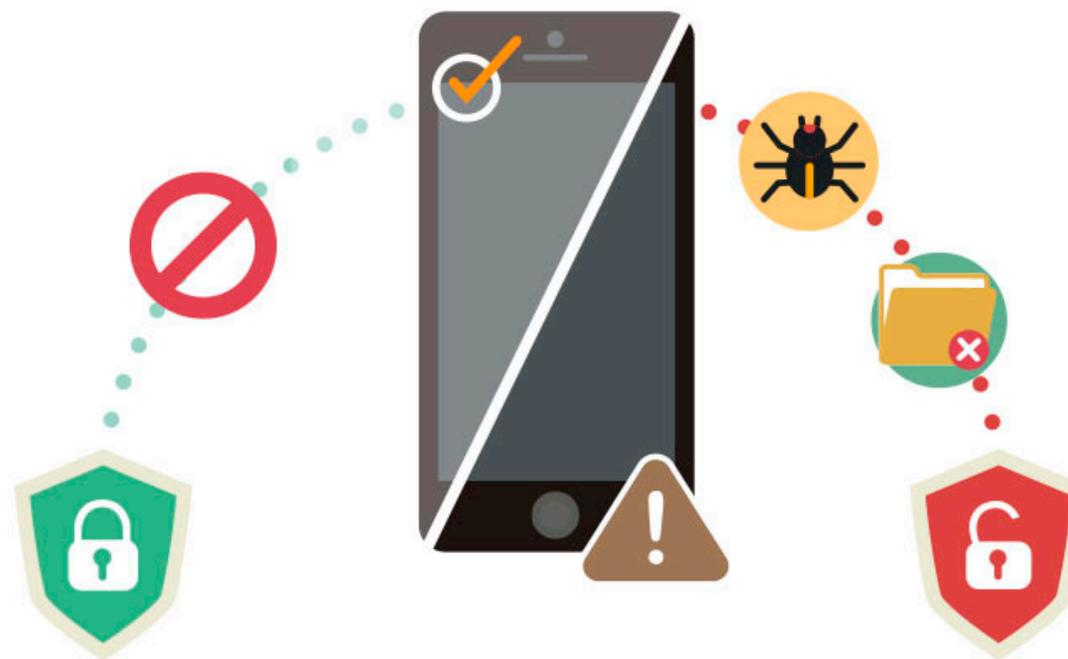
De este modo, podremos acceder con un **perfil de administrador** y **disponer de los máximos privilegios posibles**



11. ROOTING / JAILBREAKING DEL DISPOSITIVO

Aunque esto tiene un coste, y es exponernos a una **gran variedad de riesgos**:

Problemas de garantía



Infecciones por malware

Sistema menos estable



EN INCIBE TE AYUDAMOS



INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.incibe.es



TU AYUDA EN
CIBERSEGURIDAD



www.osi.es



www.is4k.es



www.incibe.es



Programas de formación



Recursos: servicios, herramientas, guías, juegos, etc.



12. Cuestionario de evaluación

Responde a la siguiente pregunta:



1. El patrón de desbloqueo de nuestra pantalla mediante el uso de nuestra huella dactilar se conoce como:

- A. Biometría.
- B. Patrón.
- C. TouchID.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



2. ¿Para qué sirven las aplicaciones de cifrado?

- A. Para detectar y eliminar posibles virus.
- B. Para cifrar todos nuestros archivos.
- C. Para mejorar el rendimiento del dispositivo.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



3. Las copias de seguridad nos permiten:

- A. Proteger la información en caso de pérdida, daño o robo.
- B. Optimizar los recursos del sistema.
- C. Mejorar la seguridad de nuestras aplicaciones.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



4. ¿Cómo se conoce a la tecnología inalámbrica que permite realizar pagos con nuestro dispositivo móvil?

- A. VPN.
- B. Google Pay.
- C. NFC.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



5. ¿Cuál de las siguientes opciones no nos sirve para identificar posibles apps maliciosas?

- A. Revisar las valoraciones de otros usuarios.
- B. Revisar si dispone de micropagos.
- C. Comprobar el número de descargas

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



6. ¿Cuál sería la postura correcta cuando una aplicación nos pide permisos antes de instalarse?

- A. No aceptar ninguno.
- B. Aceptarlos todos, si es de tienda oficial.
- C. Aceptar solo los relacionados con su función.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



7. Si almacenamos fotos o vídeos en la memoria de la tarjeta microSD que tenemos insertada en nuestro dispositivo, hablamos de:

- A. Memoria externa.
- B. Memoria interna.
- C. Memoria de terceros.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



8. De las siguientes opciones, ¿cuál no es un buen uso de la nube?

- A. Como almacén de nuestros datos más personales.
- B. Como almacén de nuestras copias de seguridad.
- C. Como almacén para liberar espacio de nuestro dispositivo.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



9. ¿Cómo se conoce al procedimiento mediante el cual podemos “liberar” nuestro dispositivo móvil?

- A. Rootingo / Freemobile.
- B. Scrooting / Jailbreacking.
- C. Rooting / Jailbreacking.

12. Cuestionario de evaluación

Responde a la siguiente pregunta:



10. ¿Cuál de los siguientes no es un riesgo vinculado a liberar nuestro dispositivo móvil?

- A. Ausencia de herramientas de protección.
- B. Problemas con la garantía
- C. Mayor riesgo de infección por malware.



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Gracias por vuestra atención



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD
incibe_



Oficina
de Seguridad
del Internauta

LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD
incibe_



Oficina
de Seguridad
del Internauta