

“VAULT APPS”: APLICACIONES PARA OCULTAR SECRETOS



Proyecto P-
45 “Audaz”



Buenas a todos ciber-navegantes. Mirad, hoy me apetece hacer algo un poco diferente. Hoy os voy a hablar de una forma de engaño de las que podéis ser víctimas, **pero que en este caso quien os engaña lo conocéis muy bien**. Porque puede ser un hijo, una hija, o una pareja sentimental... alguien que conocéis que quiera ocultar algún secreto a la vista de todo el mundo en su móvil.



Si bien en caso de mayores de edad realmente no podemos (**ni debemos**) hacer nada (porque incurriremos en un delito), esto es algo bastante peligroso cuando **lo usan menores de edad**. El motivo no es otro que en determinadas redes sociales hay una presencia mayor de personas que se pueden aprovechar de ellas para cometer delitos de **sexting, grooming** y similares, y que los animen a usar estas aplicaciones para ocultar esas actividades.

Antes de empezar hay que dejar una cosa bien clara: Cualquier persona mayor de edad tiene derecho a su privacidad y a guardar lo que considere secreto en una aplicación de este tipo. Si entras en ella para leerlo, estás incurriendo en un delito. Este documento contempla los casos en los que las usa un menor para ocultar alguna actividad ilícita, y el tutor de este debe poder actuar en consecuencia si tiene alguna sospecha

¿A qué me estoy refiriendo?

A las llamadas **aplicaciones bóveda**, aplicaciones caja fuerte o, en inglés, “**vault apps**”. Son una serie de aplicaciones que se ocultan en el móvil de formas variadas. Las menos sofisticadas intentan pasar desapercibidas, y otras más complejas **se hacen pasar por una aplicación que hace otra cosa**, como una calculadora o un juego inocente, para que nadie sepa su verdadero propósito.

El caso es que estas aplicaciones tienen un punto en el que **un usuario se puede identificar de manera especial**, ya sea con un código, una clave o incluso su huella. Y en caso de que la identificación sea positiva, te dejan ver una serie de archivos secretos que guardan, y que el usuario ha puesto ahí para que permanezcan ocultos.

Vamos, que es tu propio “cajón de secretos” en tu teléfono. Y el “cajón” (la aplicación) puede tener el aspecto de cajón o “disfrazarse” de otra cosa 😊

Y seguramente os preguntaréis *¿y no hay otra forma de ver esos archivos que a través de esa aplicación?* Pues no, porque estas aplicaciones lo que hacen es partirlos en trozos, renombrarlos, cifrarlos y/o hacerlos pasar por archivos inútiles, temporales, o simplemente que al abrirlos no tengan sentido.

 **Además algunas de ellas tienen navegadores propios, que permiten saltarse cualquier tipo de filtro de contenido que tengamos puesto en el navegador "normal" y permitir a los menores ver páginas que no tienen autorizadas. Esto las hace peligrosas en la situación que vamos a describir luego**

Y cabe decir que estas aplicaciones en sí **no son ilegales**. De hecho, poder guardar secretos en un teléfono, solo accesibles a una determinada persona que sepa cómo acceder a ellos, es una de las funcionalidades más viejas existentes y, en un contexto adecuado, muy necesaria.

 **El problema es que ahora se han hecho mucho más accesibles para menores y mucho más sencillas de usar por cualquiera, lo que abre la puerta a "malusarlas"**

¿Por qué existen?

En realidad las aplicaciones “cajas fuerte” no dejan de ser una respuesta a una necesidad muy típica, que es **guardar datos de forma segura** y oculta al ojo de cualquiera dentro de tu dispositivo móvil. Esto en sí no es nada malicioso y es muy común, especialmente si manejas información sensible o secreta en algún contexto.

El problema de estas aplicaciones es el mismo que el de tener un cuchillo. Los cuchillos se pueden usar para partir carne, y nadie puede decir nada en contra de eso. Pero el mismo cuchillo también es un arma, y si la usas contra alguien evidentemente estás cometiendo un delito. Con estas aplicaciones ocurre lo mismo: si lo usas para guardar **tus datos secretos y privados** estás en tu perfecto derecho. Voy a ponerte dos ejemplos:

1. Una persona que es **víctima de violencia de género** puede tener necesidad de ocultar pruebas de dicha violencia que haya fotografiado / grabado en este tipo de aplicaciones para poder hacer luego una denuncia. Dado que estas personas suelen estar sometidas a una **vigilancia de dispositivos extrema**, que no vean estas pruebas es imprescindible mientras consigue lo necesario para desvincularse de su agresor
2. El usuario es un **adolescente menor**, al que un *groomer* ha convencido para guardar las conversaciones que tiene con él en ese dispositivo (esto es un caso real). De esta forma, nadie pueda detectar que está manteniendo conversaciones inapropiadas siendo un menor, y la cosa cambia completamente, aunque la aplicación usada sea exactamente la misma. El *groomer* puede también usarlas para ocultar esas actividades a su familia/pareja y seguir con su apariencia de “vida normal”.

 **Ten en cuenta que el groomer va a intentar “comerle la cabeza” al menor para que cree una dependencia de él y esta ocultación de conversaciones, fotos, etc. puede ser parte de un “juego” que el groomer cree valiéndose de la confianza y la complicidad que ha adquirido con dicho menor. O quizá sea el medio para que el groomer haga al menor acceder a sitios inadecuados saltándose los filtros que su teléfono pudiera tener...**

El objetivo de este artículo es que **sepas que estas aplicaciones existen**, y que el hecho de no localizar información comprometedora en un teléfono no quiere decir que no la haya. Por tanto, si un menor a tu cargo contacta habitualmente con alguien que le ofrece usar este tipo de aplicaciones para mantener determinadas interacciones en secreto, es obvio que estamos ante un más que probable caso de un delito denunciable ante las autoridades.

 **Si al menor le informas de esto, es menos probable que sea una víctima si le llega a ocurrir, ya que tendrá una información para contrastar con lo que el groomer le diga. Es importante también que le digas que el groomer guarda una copia de estas imágenes y que luego puede usarlas para chantajearle/la, con la presión sicológica y el daño que puede hacer**

Por tanto, conocer la existencia de estas aplicaciones tiene los **objetivos** de evitar que te engañen, engañar a quien quiera leer lo que no debe leer tuyo, y prevenir que alguien convenza a una persona vulnerable para usarla para guardar lo que no debe.

¿Me puedes poner ejemplos?

Finalmente, recuerda que estas aplicaciones estás destinada a guardar información que por definición es sensible. Por tanto, **hay que extremar las precauciones a la hora de seleccionar cuál instalas**, siguiendo las precauciones habituales:

- Mirar sus **valoraciones** (media y cuántas tiene, a más, mejor)
- Consultar los **comentarios** de usuarios
- Mirar el **historial de aplicaciones del fabricante**, a ver si tiene varias en el mercado con buena reputación
- También es interesante saber si el fabricante tiene **una web oficial con buen aspecto**, que tiene acuerdos con otras empresas, que la ofrece para varias plataformas... (esto da más entidad a la empresa que hay detrás)
- Consultar **cuántas instalaciones tiene** (cuantas más menos probable es que tenga algo malicioso que nadie haya detectado)
- Mirar por Internet si hay **comentarios y valoraciones de la aplicación positivos en medios de información** fiables que hagan revisiones de ella, etc.
- Consultar **foros donde haya usuarios de estas** para ver qué opinan y los problemas que comentan
- Qué al descargarla lleven la marca de "**Verificado por Google Play Protect**", lo que implica que al menos ha pasado una revisión de seguridad básica

Como puedes ver, localizar una en *Google Play* es extremadamente fácil, solo hace falta poner "vault app" en la búsqueda (**Figura 1**). Hecho esto, nos corresponde entrar en cada una y **hacer una revisión en profundidad** antes de decidir si la instalamos o no con los criterios vistos.

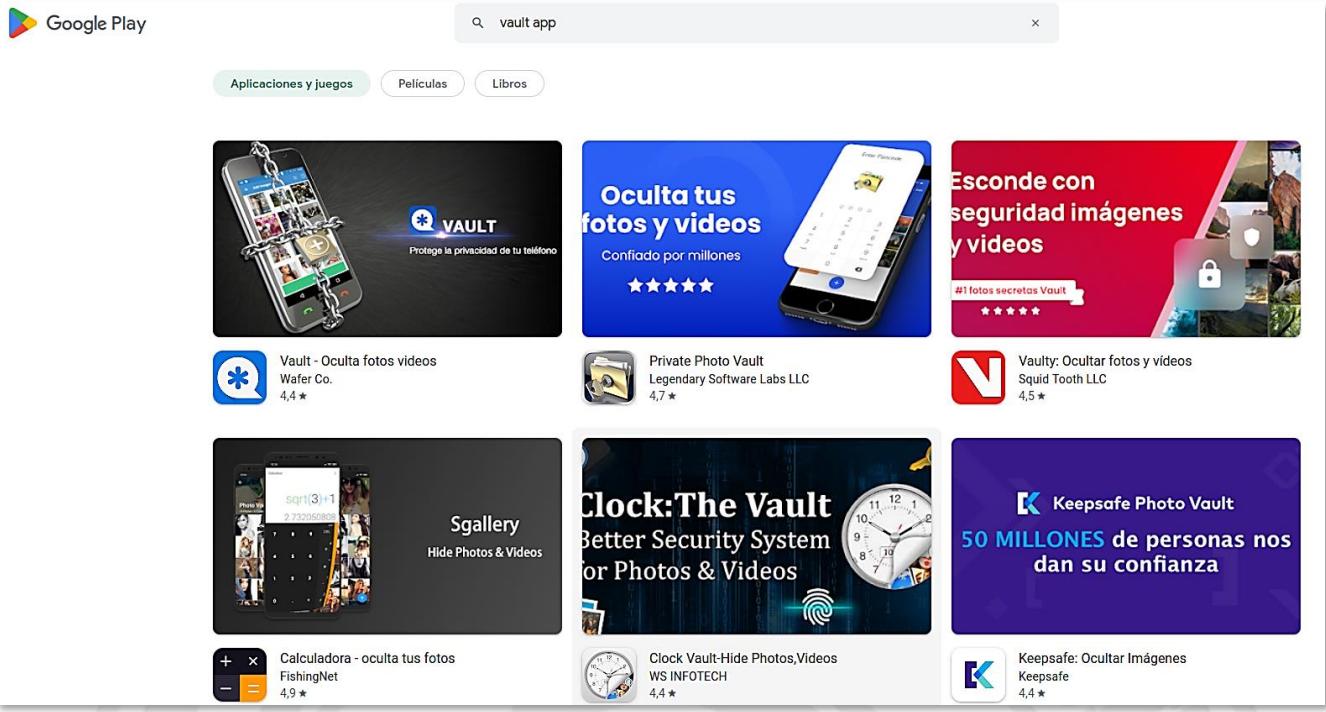


Figura 1. Localizando "vault apps" disponibles en Google Play

This screenshot shows the Google Play Store page for the 'Private Photo Vault' app. At the top, it says 'Legendary Software Labs LLC' and 'Contiene anuncios · Compras en aplicaciones'. It shows a rating of 4.7★ from 170 mil reseñas, 10 M+ descargas, and is rated for 'Para todos'. A large green 'Descargar' button is prominent. To the right is a thumbnail of the app icon, which is a padlock on a screen. Below this, there's a section titled 'Información de la aplicación' with a description: 'Private Photo Vault es una caja fuerte de seguridad para fotografías que guarda todas tus fotos y videos privados ocultos con una contraseña. ¡La aplicación para fotos privadas #1 de iOS ya está disponible en Android!'. Another section, 'Información de contacto del desarrollador', is partially visible. On the right side, there's a 'Aplicaciones similares' section with links to other apps like 'Calculator Lock - Hide Photos', 'Bloquear: ocultar foto y video', 'LockMyPix Ocultar Fotos Vídeos', and 'Ocultar Fotos & Videos: Pinbox'.

Figura 2. Private Photo Vault es una aplicación de esta clase especializada en fotos. Fuente: https://play.google.com/store/apps/details?id=com.enchantedcloud.photovault&hl=en_US

Fíjate en las que hay en las siguientes imágenes (**Figura 3, Figura 4 y Figura 5**) y la enorme diferencia que hay entre su nº de opiniones, valoración y descargas. También debes tener en cuenta **si sus funcionalidades te convienen**, puesto que pueden estar limitadas.

💡 Por favor, ten en cuenta que **yo no puedo recomendarte ninguna porque no las uso**, pero te estoy dando los criterios de selección adecuados para que lo hagas tú. Estos criterios los puedes aplicar también sobre cualquier aplicación que quieras instalar, ¡no solo vault apps! 😊

Vault - Oculta fotos videos

Wafer Co.

Contiene anuncios · Compras directas desde la app

4.3★

1.29 M opiniones

100 M+

Descargas



Apto para todo público

Instalar

Compartir

Agregar a la lista de deseos



Figura 3. Aplicación Vault- Oculta fotos videos. Fuente: https://play.google.com/store/apps/details?id=com.netqin.ps&hl=es_419&gl=US

Calculator# Lock Hide Gallery

NewSoftwares LLC

Contains ads · In-app purchases

4.3★

4.18K reviews

100K+

Downloads



PEGI 3

Install

Share

Add to wishlist



Figura 4. Aplicación Calculator# Lock Hide Gallery. Esta es una de las que se hacen pasar por otra cosa. Fuente: <https://play.google.com/store/apps/details?id=net.newsoftwares.hidepicturesvideos&hl=en>

Calculator Vault - Hide Photos

Vasundhara Infotech LLC
Contains ads · In-app purchases

4.6★ 27.5K reviews 1M+ Downloads PEGI 3

Install

Share

Add to wishlist

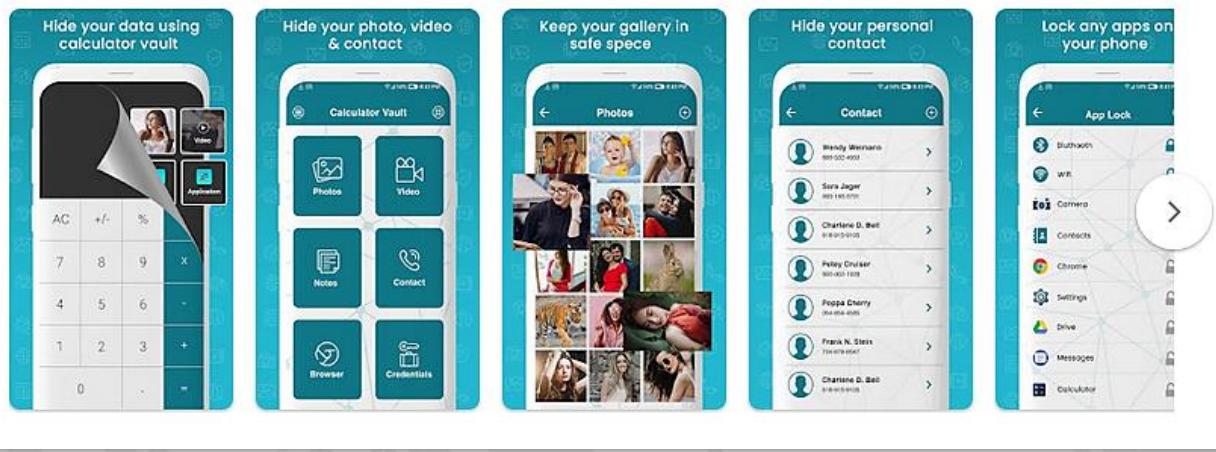


Figura 5. Aplicación Calculator Vault- Hide fotos. Fuente:
<https://play.google.com/store/apps/details?id=com.calculator.vault.gallery.locker.hide.data&hl=en>

¿Me puedes dar criterios más avanzados para decidir si me instalo una o no?

Dada la delicadeza de la información que van a contener estas aplicaciones, te doy aquí más criterios detallados para que tomes una decisión informada.

Puedes por ejemplo instalarla en un teléfono viejo que hayas vaciado y que ya no uses para hacerle pruebas antes de pasarlo a tu teléfono principal.

Utilidad y necesidad:

- ¿La aplicación resuelve un problema real o satisface una necesidad específica que tienes?
- ¿Aporta valor a tu vida diaria o actividades profesionales?
- ¿Existen otras aplicaciones similares que ya usas y que podrían cubrir la misma función?

Funcionalidad y características:

- ¿La aplicación ofrece las funciones que necesitas y las hace de manera efectiva?
- ¿Es fácil de usar y tiene una interfaz intuitiva?
- ¿Está disponible en tu idioma y es compatible con tu dispositivo?

Confiabilidad y seguridad:

- ¿La aplicación proviene de un desarrollador confiable y con buena reputación?

- ¿Tiene buenas críticas y valoraciones de otros usuarios?
- ¿Solicita permisos excesivos o acceso a datos sensibles? (puedes verlo en su ficha de Google Play o como veremos después)
- ¿Cuenta con políticas de privacidad claras y transparentes? (puedes verlo en su ficha de Google Play)

Popularidad y soporte:

- ¿La aplicación tiene una base de usuarios activa y una comunidad sólida?
- ¿Recibe actualizaciones frecuentes con mejoras y correcciones de errores?
- ¿Cuenta con soporte técnico en caso de que tengas problemas?

Privacidad y seguridad:

- ¿La aplicación recopila datos personales? Si es así, ¿cómo los utiliza y protege?
- ¿Comparte tus datos con terceros? (rastreadores, que veremos a continuación)
- ¿Ofrece opciones para controlar la configuración de privacidad?

Consideraciones adicionales:

- **Precio:** ¿La aplicación es gratuita o requiere una suscripción o compra? ¿Las compras dentro de la aplicación son razonables?
- **Batería y rendimiento:** ¿La aplicación consume mucha batería o afecta el rendimiento de tu dispositivo?
- **Opiniones y reseñas:** ¿Qué dicen otros usuarios sobre la aplicación? ¿Hay comentarios negativos recurrentes que debes tener en cuenta?

Uso de permisos y rastreadores:

El uso de permisos de la aplicación depende mucho de lo que haga, por lo que es difícil decidir si son muchos o pocos sin conocimientos técnicos. **No obstante, cuantos menos, mejor.** Lo que si es importante es el uso de rastreadores, que son elementos del programa que **analizan lo que hacemos con él** (y otros comportamientos) y los venden a empresas de publicidad para servirnos anuncios técnicamente más adaptados a nuestros gustos.

 Antes de que creas que esto es una práctica ilegal, no lo es. Muchas de estas aplicaciones son gratuitas en precio, pero realmente el uso de los datos que obtienen tras analizar tus comportamientos con rastreadores y su posterior venta es su forma de ganar dinero. ¡Los programadores tienen que comer! 😊 Además, al instalarlas consientes a que lo hagan...

¿Y cómo puedes saber cuántos rastreadores usa una aplicación de forma fácil y sencilla? Gracias a la web **Exodus Privacy** (<https://reports.exodus-privacy.eu.org/es/>) (Figura 6).

**exodus**La plataforma de auditoría de privacidad para
aplicaciones Android**Buscar un informe**

Nombre de la aplicación



Puede buscar una aplicación usando su nombre, gestor o URL de Google Play
ej: Meteo France o fr.meteo o <https://play.google.com/store/apps/details?id=fr.meteo>
¿No puede encontrar la aplicación? Busque en [Google Play](#).

¡Vamos!

Buscando una aplicación que aún no conocemos?

Realizar un nuevo análisisexodus analiza las aplicaciones Android para **listar los rastreadores integrados**.

Un rastreador es una pieza de software **destinada a recopilar datos sobre ti o tus usos**. Así que,
los informes exodus te dicen cuáles son los ingredientes del pastel.

exodus no descompila aplicaciones, su método de análisis es legal.

Figura 6. Esta es Exodus Privacy, tu web para "diseccionar" aplicaciones de móvil 😊

Si ahora analizamos tres de las aplicaciones anteriores tenemos, como se puede ver en las figuras siguientes, un resultado muy dispar en cuanto a permisos y rastreadores (**cuantos menos de ambos, ¡mejor! 😊**)

🔍 **Para analizar las aplicaciones basta con que metas la dirección de esta en Google Play (hay muchas con un nombre parecido y hacerlo con el nombre es confuso). Puedes mismamente poner el enlace que te pongo en el pie de foto. Para otras, puedes buscarlas en la versión web de Google Play simplemente (<https://play.google.com/store/>).**

exodus

Inicio Informes Rastreadores Entender mejor La organización

es

exodus v1.28



Vault

12 rastreadores **44 permisos**

Versión 6.9.11.62.22 - [ver otras versiones](#)
 Fuente: Google Play
 Informe creado el 13 de Octubre de 2023 a las 19:56 y actualizado el 5 de Diciembre de 2023 a las 11:31
[Ver en Google Play >](#)

12 rastreadores

Hemos encontrado firma de código de los siguientes rastreadores en la aplicación:

- AdColony > [advertisement](#)
- Amazon Advertisement >
- AppLovin (MAX and SparkLabs) > [analytics](#) [profiling](#) [identification](#) [advertisement](#)
- Facebook Ads > [advertisement](#)
- Facebook Analytics > [analytics](#)
- Google AdMob > [advertisement](#)
- Google Crashlytics >

Figura 7. Rastreadores y permisos de Vault

exodus

Inicio Informes Rastreadores Entender mejor La organización

es



Calculator

3 rastreadores **18 permisos**

Versión 1.1.2 - [ver otras versiones](#)
 Fuente: Google Play
 Informe creado el 14 de Marzo de 2020 a las 15:35 y actualizado el 9 de Diciembre de 2023 a las 06:51
[Ver en Google Play >](#)

3 rastreadores

Hemos encontrado firma de código de los siguientes rastreadores en la aplicación:

- Google AdMob > [advertisement](#)
- Google Analytics > [analytics](#)
- Google Tag Manager > [analytics](#)

Un rastreador es un software destinado a recopilar datos sobre ti o tus usos. [Aprende más...](#)

18 permisos

Hemos encontrado los siguientes permisos en la aplicación:

- ACCESS_NETWORK_STATE
view network connections
- ACCESS_WIFI_STATE

Figura 8. . Rastreadores y permisos de Calculator #



Calculator

14 rastreadores**24 permisos**Versión 3.4 - [ver otras versiones](#)

Fuente: Google Play

Informe creado el 14 de Marzo de 2020 a las 15:42 y actualizado el 9 de Diciembre de 2023 a las 06:51

[Ver en Google Play >](#)**14 rastreadores**

Hemos encontrado firma de código de los siguientes rastreadores en la aplicación:

AdColony >

[advertisement](#)

AppLovin (MAX and SparkLabs) >

[analytics](#) [profiling](#) [identification](#) [advertisement](#)

Appnext >

ChartBoost >

Facebook Ads >

[advertisement](#)

Google AdMob >

[advertisement](#)

Google CrashLytics >

[crash reporting](#)

Google Firebase Analytics >

Figura 9. . Rastreadores y permisos de Calculator. Si tienes dudas de cual es, siempre puedes hacer clic en "Ver en Google Play" para comprobar que es exactamente la que estás estudiando

 Recuerda que lo más importante es que la aplicación te aporte valor y satisfaga tus necesidades. No te dejes llevar por las modas o las aplicaciones con mayor número de descargas. Analiza cuidadosamente las características y funcionalidades que ofrece cada app, y prioriza aquellas que realmente te sean útiles.

Y como siempre que termino menciono contramedidas, este informe no va a ser una excepción. El problema es que la medida no es probablemente la que algunos podrían esperar. Estas aplicaciones **no son ilegales ni son un delito** y algunas son extremadamente difíciles de detectar porque están creadas para contener secretos. Por tanto, la única medida de seguridad que realmente funciona es **mantener una comunicación con nuestros menores a cargo, dar confianza** y explicar muy detalladamente los peligros que tiene intercambiar determinado tipo de materiales y, sobre todo, el daño que se le puede hacer tanto a uno mismo como a los demás si se fomenta el compartir material privado, denigratorio o sensible de otras personas, como he dicho anteriormente.

Y este es uno de los casos en los que la tecnología ha avanzado tanto que, en mi opinión, la única contramedida que realmente funciona no es ni la prohibición ni la eliminación **sino la concienciación y fomentar el sentido común**.

Y finalmente un poco lo de siempre. Por favor, **cuéntaselo a la gente** porque esto es algo que no sabe mucha gente, y nunca sabes cuando alguien que conozcas puede verse en un problema como los descritos. **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, tener secretos está bien, ¡el problema es cuando alguien engaña a un menor para ocultar las pruebas de un delito!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)
- [Escúchalo en mi canal de YouTube](#)
- [¿Tienes otro cliente de Podcast? Este es el feed RSS](#)

¿Quieres leer alguna noticia/artículo relacionado?



- [Las 7 mejores aplicaciones para hacer fotos de forma segura en 2023 \(04/01/2023\)](#)
- [Cinco aplicaciones "tapadera" que no son lo que dicen ser para guardar tus fotos, vídeos y aplicaciones \(02/2023\)](#)
- [Cómo esconder apps en la calculadora de tu Android: esta app lo hace posible \(13/07/2021\)](#)

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 08/05/2023

² Algunas imágenes del texto del documento han sido generadas con la IA Bing Chat