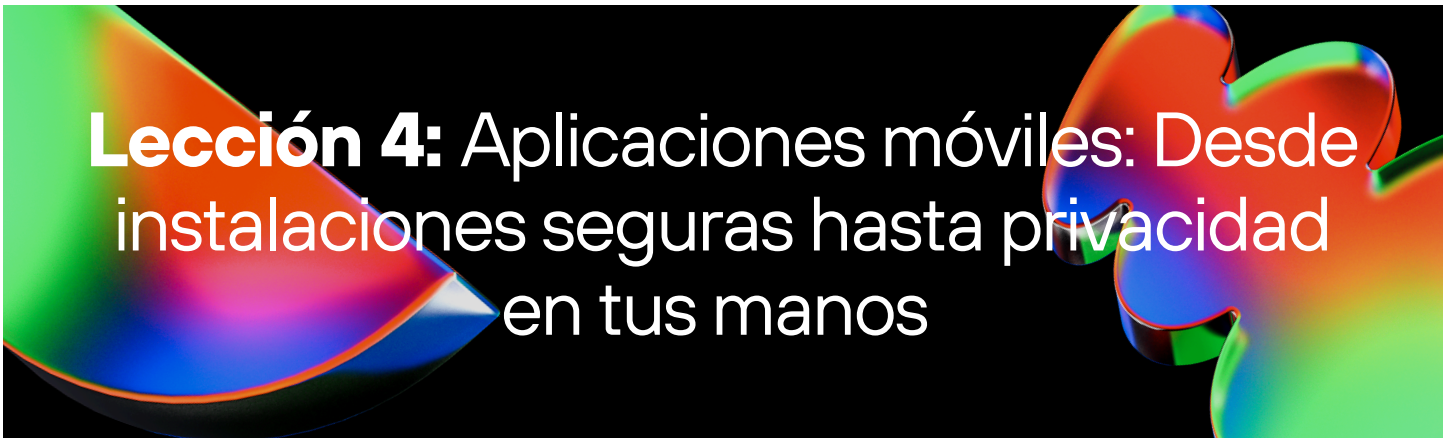
Protejeres

Programa Tejiendo Redes Seguras




## Objetivo

Promover el manejo adecuado de la privacidad y la instalación segura de aplicaciones móviles, abordando categorías, procedimientos de descarga e instalación, así como aspectos clave de seguridad digital.

# Introducción a las aplicaciones móviles

Las aplicaciones móviles, comúnmente conocidas como "apps", son programas diseñados específicamente para funcionar en dispositivos móviles, como teléfonos inteligentes 📱 y tabletas. Estas aplicaciones pueden ser descargadas e instaladas desde tiendas virtuales como **Google Play Store** para dispositivos Android o **App Store** para dispositivos iOS.

## Relevancia en la vida cotidiana

Las aplicaciones móviles son como 🌟 estrellas en el universo digital 📱. Ofrecen un mundo de posibilidades 🌎, desde mantenernos conectados con amigos y familiares con apps como WhatsApp y Messenger 📲, hasta gestionar nuestras finanzas con aplicaciones bancarias móviles 💰. ¡La variedad es infinita! 🚀

Imagina poder acceder a entretenimiento, productividad, educación, salud, finanzas, ¡y mucho más! Todo al alcance de tu mano con solo unos toques en la pantalla 🎮📚💊💳.

La relevancia de estas aplicaciones en nuestra vida diaria es innegable. Son como 🎁 regalos que hacen nuestra vida más fácil y emocionante. Nos ofrecen soluciones a medida que se adaptan a nuestras necesidades y preferencias personales 🤩.

Y lo mejor de todo es su comodidad, accesibilidad y portabilidad. Las llevamos con nosotros a donde quiera que vayamos, convirtiéndose en compañeras indispensables en nuestro día a día 🌟.

## Aplicaciones móviles que han transformado diferentes aspectos de la sociedad

**Comunicación:** Aplicaciones como WhatsApp, Telegram y Skype han cambiado la forma en que nos comunicamos, permitiéndonos enviar mensajes

de texto, hacer llamadas de voz y video, compartir archivos multimedia y más, todo de forma gratuita o a un costo mínimo.

**Entretenimiento:** Plataformas de transmisión de contenido como Netflix, Spotify y YouTube ofrecen acceso instantáneo a una amplia gama de contenido multimedia, desde películas y series de televisión hasta música y videos, que pueden ser disfrutados en cualquier momento y lugar.

**Productividad:** Aplicaciones de productividad como Microsoft Office, Google Workspace y Trello facilitan la organización y colaboración en proyectos, permitiendo a los usuarios crear y editar documentos, gestionar tareas y programar reuniones desde sus dispositivos móviles.

**Educación:** Plataformas de aprendizaje en línea como Coursera, Khan Academy y Duolingo ofrecen acceso a una amplia variedad de cursos y materiales educativos, permitiendo a los usuarios aprender nuevas habilidades y ampliar sus conocimientos desde la comodidad de sus dispositivos móviles.

## ¿Riesgos a la hora del uso de Apps?

**Privacidad de los datos:** Son varias las aplicaciones que recopilan información personal del usuario, como la ubicación, la información de contacto y los hábitos de navegación. Si esta información se recopila sin el consentimiento del usuario o se comparte con terceros de manera no autorizada, puede comprometer la privacidad del usuario.

¿Por esto Facebook o Google me recomiendan algo que buscaba?

---

**Sí,** los permisos que otorgas a aplicaciones como Google o Facebook **pueden influir en su capacidad para recomendarte cosas basadas en tus conversaciones u otras actividades en línea**. Aunque estas empresas generalmente afirman que no escuchan activamente tus conversaciones, **utilizan algoritmos y tecnologías de análisis de datos para recopilar información sobre tus intereses, comportamientos y preferencias.**

**De esta manera Google, Facebook y otras empresas pueden utilizar tus datos para recomendarte cosas.**

# ¿Cuál es el proceso de recolección de información?

**1. Análisis de contenido:** Google y Facebook pueden analizar el contenido de tus correos electrónicos, mensajes, publicaciones y comentarios para comprender tus intereses, preferencias y necesidades.

Pueden identificar palabras clave o temas recurrentes en tus conversaciones para ofrecerte anuncios relevantes o contenido personalizado.

2. **Seguimiento de actividad:** Estas empresas también pueden rastrear tu actividad en línea, como las búsquedas que realizas, los sitios web que visitas y los productos que compras.

Utilizan esta información para crear perfiles de usuario detallados y ofrecerte recomendaciones personalizadas de productos, servicios o contenido.

**3. Datos de ubicación:** Si les has otorgado permiso para acceder a tu ubicación, Google y Facebook pueden utilizar esta información para ofrecerte recomendaciones basadas en tu ubicación actual o hábitos de viaje.

Por ejemplo, podrían recomendarte restaurantes cercanos, eventos locales o tiendas cercanas.

**4. Historial de compras**: Si has utilizado servicios como Google Pay o Facebook Marketplace para realizar compras, estas empresas pueden utilizar tu historial de compras para recomendarte productos o servicios relacionados en el futuro.

Es importante tener en cuenta que estas prácticas de recopilación de datos y recomendación se realizan en gran medida a través de algoritmos automatizados.

Las empresas pueden utilizar una variedad de fuentes de datos, incluidos tus correos electrónicos, mensajes y publicaciones, para comprender mejor tus intereses y necesidades.

Para proteger tu privacidad y controlar la cantidad de información que estas empresas pueden recopilar sobre ti, puedes revisar y ajustar la configuración de privacidad en tus cuentas de Google y Facebook, así como limitar los permisos que otorgas a las aplicaciones en tus dispositivos. Además, puedes utilizar herramientas como la navegación privada o los bloqueadores de anuncios para limitar la cantidad de datos que estas empresas pueden recopilar mientras navegas por internet.

## ¿Pero que son los permisos?

Los permisos son autorizaciones que otorgas a una aplicación para acceder a ciertas funciones, datos o recursos en tu dispositivo o en línea. Cuando instalas una aplicación en tu dispositivo móvil, tableta o computadora, generalmente se te solicitará que otorgues permisos específicos para que la aplicación funcione correctamente.

Estos permisos pueden variar según la plataforma y el tipo de aplicación, pero generalmente incluyen cosas como acceso a la cámara, micrófono, ubicación, contactos, almacenamiento, conexión a internet y otros recursos del dispositivo. Por ejemplo:

1. **Permiso de ubicación**: Permite que la aplicación acceda a la ubicación actual de tu dispositivo. Esto se utiliza comúnmente en aplicaciones de mapas, navegación, clima y redes sociales para proporcionar servicios basados en la ubicación.
2. **Permiso de cámara y micrófono**: Permite que la aplicación tome fotos, grabe videos o capture audio utilizando la cámara y el micrófono de tu dispositivo. Esto se utiliza en aplicaciones de redes sociales, videollamadas, grabadoras de voz, entre otros.
3. **Permiso de contactos**: Permite que la aplicación acceda a tu lista de contactos para que puedas enviar mensajes, realizar llamadas o invitar a amigos a usar la aplicación.
4. **Permiso de almacenamiento**: Permite que la aplicación acceda a los archivos almacenados en tu dispositivo, como fotos, videos, música y

documentos. Esto se utiliza para cargar archivos, descargar contenido o acceder a datos guardados en el dispositivo.

5. **Permiso de conexión a internet**: Permite que la aplicación se conecte a internet para acceder a contenido en línea, enviar y recibir datos, y sincronizarse con servidores remotos.

ES IMPORTANTE TENER EN CUENTA QUE **OTORGAR PERMISOS A UNA APLICACIÓN SIGNIFICA QUE ESTÁS PERMITIENDO QUE ACCEDA A CIERTA INFORMACIÓN O FUNCIONALIDAD** EN TU DISPOSITIVO. POR LO TANTO, ES FUNDAMENTAL REVISAR CUIDADOSAMENTE LOS PERMISOS QUE SOLICITA UNA APLICACIÓN ANTES DE INSTALARLA Y CONSIDERAR SI **ESTÁS CÓMODO CON LA INFORMACIÓN A LA QUE LA APLICACIÓN TENDRÁ ACCESO**

## ¿Cómo podemos cuidar nuestra privacidad?

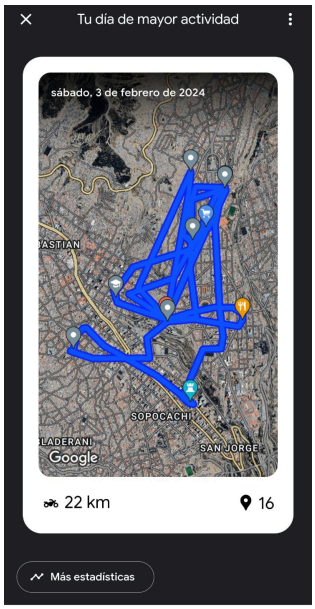
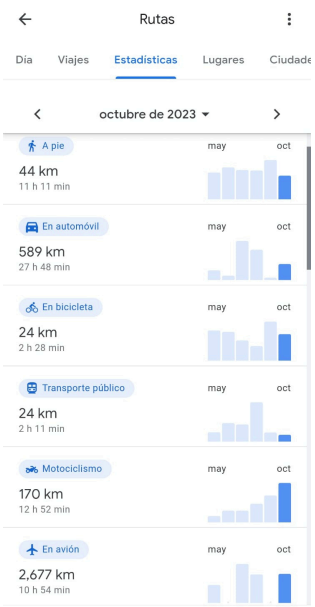
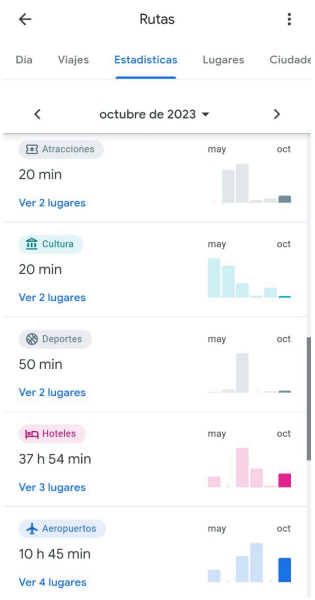
Aquí hay algunas formas en que las aplicaciones pueden recopilar información personal y cómo podría comprometerse la privacidad del usuario:

1. Permisos de la aplicación: Al instalar una aplicación, generalmente se solicitan permisos que la aplicación necesita para funcionar correctamente.

Si el usuario otorga estos permisos sin darse cuenta o sin comprender completamente cómo se utilizará la información, la aplicación puede recopilar datos personales sin su consentimiento explícito.

2. Seguimiento de la ubicación: Muchas aplicaciones solicitan acceso a la ubicación del dispositivo del usuario para proporcionar servicios basados en la ubicación, como mapas, recomendaciones locales, etc. Si una aplicación rastrea continuamente la ubicación del usuario sin su conocimiento o consentimiento, podría revelar detalles sobre los movimientos y hábitos del usuario, lo que podría comprometer su privacidad.

Aplicaciones como GoogleMaps, desde el momento de la activación del dispositivo móvil Android empiezan un proceso de recolección de información del usuario. Desde los recorridos que se realizan, hasta los lugares que se visitan, el tipo de movilidad empleado y el tiempo de permanencia.

| **Rutas y lugares visitados** | **Tipo de movilidad empleado** | **Permanencia o tiempo dedicado a una actividad física o de esparcimiento** | **Informe de viajes y rutas realizadas** |
|---|---|---|---|
|  |  |  |  |









**Estos datos están disponibles en cada dispositivo Android con una cuenta de Google vinculada**

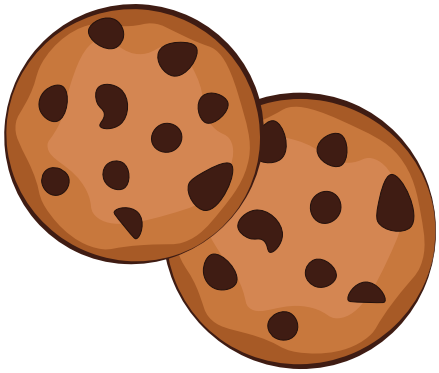
**3. Recopilación de datos de navegación:** Algunas aplicaciones pueden recopilar información sobre los sitios web que visita el usuario, las búsquedas que realiza y otras actividades en línea.

## ¿Cómo se recopilan los datos en línea?

**Mediante tecnologías de seguimiento y análisis que muchas aplicaciones utilizan para recopilar datos** sobre las actividades en línea de los usuarios.

Aquí hay una explicación 🧠 más detallada de cómo funciona 🤯:

**1. Seguimiento de actividad:** Las aplicaciones pueden integrar códigos de seguimiento, como cookies, píxeles de seguimiento, SDK (kits de desarrollo de software) y otras tecnologías similares, en sus plataformas.

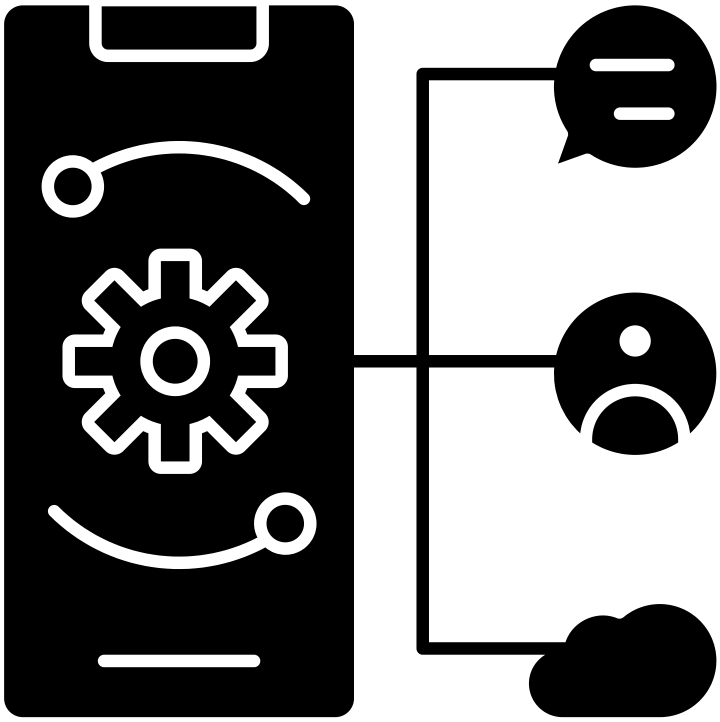


Estas tecnologías permiten a las aplicaciones registrar las acciones de los usuarios, como las **páginas web que visitan, las búsquedas que realizan, las interacciones en las redes sociales y otras actividades en línea.**

**2. Recopilación de datos:** Una vez que se ha implementado el seguimiento de actividad, las aplicaciones recopilan datos sobre el comportamiento del usuario en línea.

Estos datos pueden incluir información sobre las **páginas web visitadas, las consultas de búsqueda realizadas, los productos vistos, los clics en anuncios** y más.

**3. Análisis de datos:** Después de recopilar los datos, las aplicaciones utilizan algoritmos y técnicas de análisis de datos para procesar la información y extraer patrones y tendencias.



Incluyendo la identificación de intereses, preferencias, comportamientos de compra y otros datos relevantes sobre el usuario.

**4. Falta de seguridad de datos:** Si los datos personales recopilados por una aplicación no se almacenan o se transmiten de manera segura, podrían estar expuestos a ataques de hackers o violaciones de seguridad.

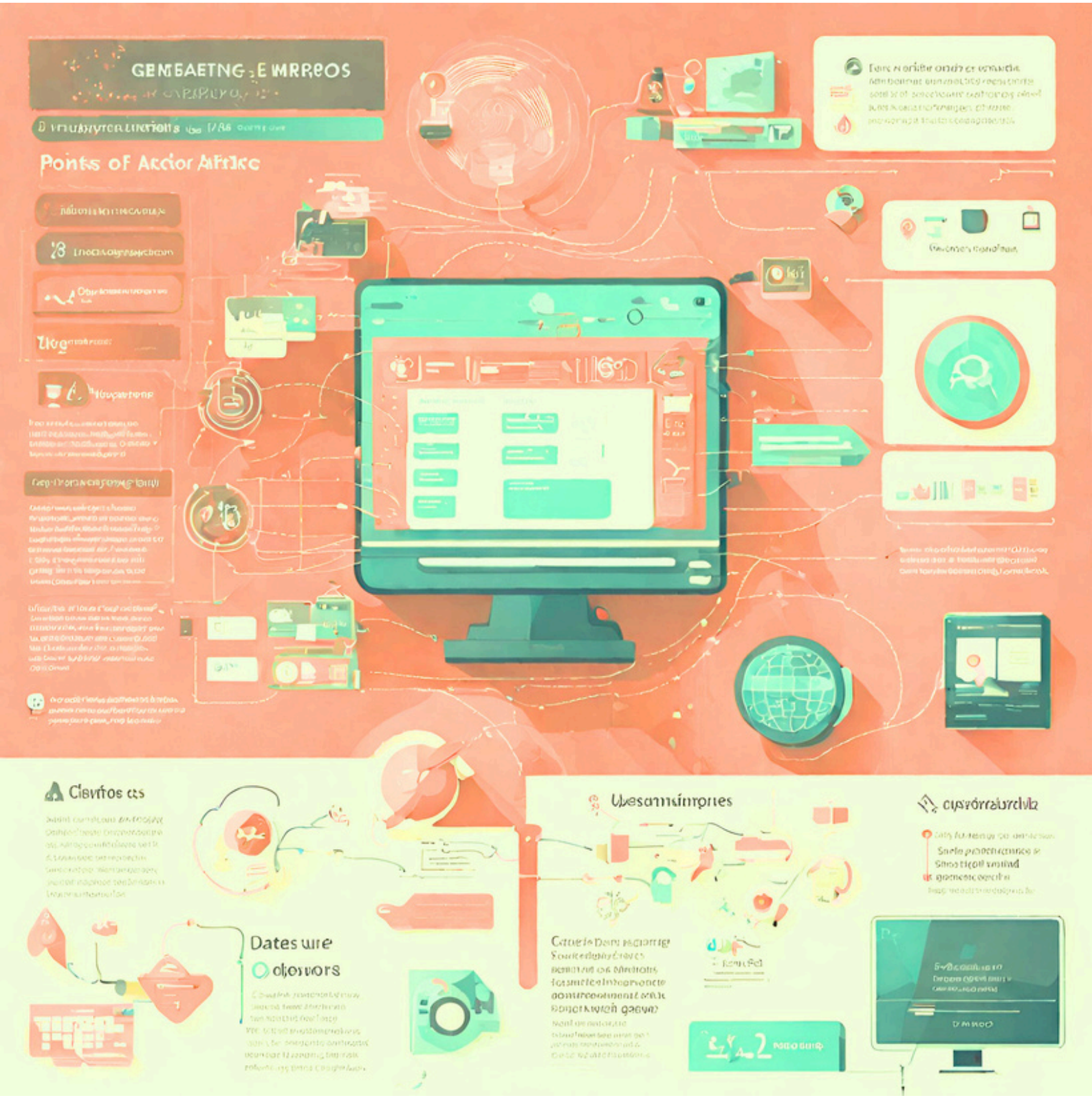
Esto podría resultar en la exposición de **información sensible del usuario**, como contraseñas, información financiera o datos de tarjetas de crédito.

Por ello, es importante que **los usuarios sean conscientes de cómo las aplicaciones recopilan y utilizan su información personal**, y que revisen las políticas de privacidad y los permisos de las aplicaciones antes de instalarlas.

# Cuidado con la seguridad de los datos

Las aplicaciones pueden ser vulnerables a ataques de hackers o brechas de seguridad, lo que puede resultar en la **exposición de datos sensibles del usuario**, como contraseñas, información financiera o datos de tarjetas de crédito.

Aquí hay algunas formas en que esto puede suceder:



1. **Errores de programación:** Los desarrolladores pueden cometer errores al escribir el código de una aplicación, lo que puede dejar vulnerabilidades en el software que podrían ser explotadas por hackers.
2. **Falta de actualizaciones de seguridad:** Si los desarrolladores no actualizan regularmente la aplicación para abordar nuevas vulnerabilidades o parchear errores conocidos, la aplicación puede quedar expuesta a ataques que aprovechan esas vulnerabilidades.
3. **Dependencia de bibliotecas o frameworks no actualizados:** Muchas aplicaciones dependen de bibliotecas de terceros o frameworks para ciertas funcionalidades. Si estas bibliotecas no se actualizan regularmente para corregir fallos de seguridad conocidos, la aplicación puede ser vulnerable a ataques que exploten esas vulnerabilidades.
4. **Almacenamiento inseguro de datos:** Si una aplicación almacena datos sensibles, como contraseñas o información financiera, de manera insegura en el dispositivo o en servidores remotos, esos datos pueden ser comprometidos si un hacker logra acceder a ellos.
5. **Fuerza bruta y ataques de diccionario:** Algunas aplicaciones pueden ser vulnerables a ataques de fuerza bruta o de diccionario, donde un hacker intenta adivinar contraseñas o credenciales de usuario mediante el uso de programas automatizados que prueban diferentes combinaciones de contraseñas.
6. **Ingeniería social:** Los hackers también pueden aprovechar la ingeniería social para engañar a los usuarios y obtener acceso a sus datos sensibles. Esto puede incluir técnicas como el phishing, donde los usuarios son engañados para que revelen información confidencial a través de correos electrónicos falsificados o sitios web fraudulentos.

**Es importante que los desarrolladores tomen medidas para proteger sus aplicaciones** y que los usuarios sean conscientes de los riesgos y tomen medidas para proteger sus datos sensibles.

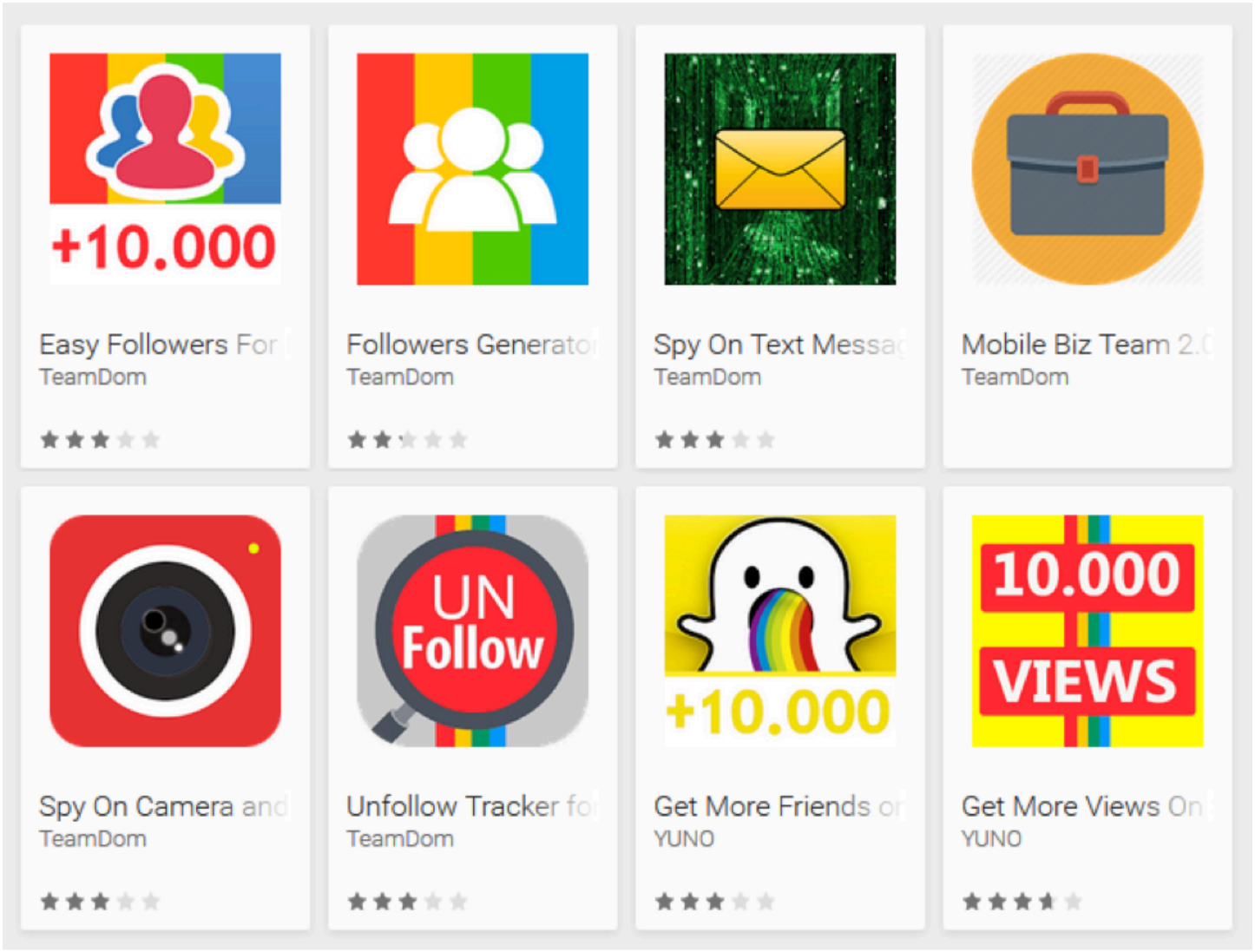
## Malware y software no deseado

Algunas aplicaciones pueden contener malware o software no deseado que puede dañar el dispositivo, robar información o realizar actividades maliciosas sin el conocimiento del usuario.

Aquí hay algunas formas en que el malware y el software no deseado pueden infiltrarse en las aplicaciones:

**1. Descargas desde fuentes no confiables:** Si descargas aplicaciones desde fuentes no oficiales o no confiables, como sitios web de terceros o tiendas de aplicaciones no verificadas, corres un mayor riesgo de descargar aplicaciones que contienen malware o software no deseado.

**2. Aplicaciones falsas o piratas:** Algunas veces, los desarrolladores malintencionados crean versiones falsas de aplicaciones populares y las distribuyen en línea. Estas aplicaciones falsas pueden contener malware o adware que se instala en tu dispositivo cuando descargas e instalas la aplicación.




Hay aplicaciones tipo anzuelo, que te **ofrecen ganar seguidores,** o **recientemente ganar dinero**, pero únicamente son para ingresar al dispositivo e instalar un malware o adware.

| Malware | Adware |
| --- | --- |
| Malware es un término general que engloba cualquier tipo de software malicioso diseñado para dañar, alterar o tomar el control de un sistema informático sin el consentimiento del usuario. | El adware es un tipo específico de software que muestra anuncios no deseados en un dispositivo, generalmente en forma de ventanas emergentes, banners o redirecciones a sitios web publicitarios. |

Incluso cuando las aplicaciones provienen de fuentes aparentemente **confiables como Google Play,** el riesgo de descargar aplicaciones maliciosas sigue siendo significativo. La presencia de código malicioso integrado en

bibliotecas de terceros demuestra que incluso las plataformas de distribución de aplicaciones más grandes no son inmunes a las amenazas de seguridad. Por lo tanto, **los usuarios deben ser cautelosos al descargar aplicaciones,** verificar los permisos que solicitan y revisar las reseñas y calificaciones de otras personas antes de instalar cualquier aplicación, i**ncluso si proviene de una tienda de aplicaciones conocida**. La conciencia y la precaución son fundamentales para proteger la seguridad y la privacidad de los usuarios en el entorno digital en constante evolución.

## Adware y casos registrados

Otro caso, pero adware, donde se registraron un total de 451 millones de descargas en **Google Play** relacionadas con aplicaciones que ofrecían anuncios de minijuegos y recopilación de datos. El caso más significativo ocurrió en mayo de 2023, cuando un equipo de investigadores identificó 101 aplicaciones que no cumplían con los criterios de elegibilidad de Google Play. Estas aplicaciones acumularon un total de **421 millones de descargas**, y cada una de ellas contenía una biblioteca con el código SpinOk, un software malicioso.

Posteriormente, otro equipo de investigadores descubrió 92 aplicaciones adicionales en Google Play que también integraban la **biblioteca SpinOk**. Aunque estas aplicaciones tenían un número de descargas menor, con un total de **30 millones**, el número combinado de aplicaciones afectadas ascendió a casi 200. En conjunto, estas aplicaciones alcanzaron las 451 millones de descargas desde **Google Play**.

Este caso evidencia otra instancia en la que se insertó código peligroso en aplicaciones a través de una biblioteca de terceros. Aparentemente, estas aplicaciones estaban destinadas a mostrar minijuegos intrusivos con promesas de recompensas en efectivo. Sin embargo, la biblioteca **SpinOk** tenía la capacidad adicional de recopilar y enviar datos y archivos del usuario al servidor de mando y control de sus desarrolladores en segundo plano.

En ese sentido, incluso cuando las aplicaciones provienen de fuentes aparentemente confiables como **Google Play,** el riesgo de descargar aplicaciones maliciosas sigue siendo significativo. La presencia de código malicioso integrado en bibliotecas de terceros demuestra que incluso las

plataformas de distribución de aplicaciones más grandes no son inmunes a las amenazas de seguridad.

Por lo tanto, los usuarios deben ser cautelosos al descargar aplicaciones, verificar los permisos que solicitan y revisar las reseñas y calificaciones de otras personas antes de instalar cualquier aplicación, incluso si proviene de una tienda de aplicaciones conocida. La conciencia y la precaución son fundamentales para proteger la seguridad y la privacidad de los usuarios en el entorno digital en constante evolución.

**3. Actualizaciones maliciosas:** Incluso las aplicaciones legítimas pueden ser comprometidas si un atacante logra infiltrarse en los servidores de la empresa o si el desarrollador original es descuidado con la seguridad. En estos casos, un atacante podría distribuir actualizaciones maliciosas que contienen malware a los usuarios que ya tienen la aplicación instalada.

**Ejemplo**

**iRecorder,** una aplicación de grabación de pantalla para teléfonos Android, subida a Google Play en septiembre de 2021, se convirtió en una amenaza cuando sus desarrolladores agregaron funcionalidad maliciosa en agosto de 2022. Incorporaron el código del troyano de acceso remoto AhMyth, que activaba el micrófono de los dispositivos cada 15 minutos, grabando audio que luego se enviaba al servidor de los creadores de la app. Este software malicioso pasó desapercibido hasta mayo de 2023, cuando los investigadores lo descubrieron. Para entonces, la aplicación había sido descargada más de 50,000 veces.

Según los investigadores de **Kaspersky**, este caso ilustra cómo las aplicaciones maliciosas pueden eludir las medidas de seguridad de **Google Play**. Inicialmente, los ciberdelincuentes publican una aplicación inofensiva que pasa los controles de moderación. Luego, una vez que la aplicación gana una base de usuarios y cierta reputación, se actualiza con funcionalidades maliciosas.