



Ya comenzó el despliegue de verificación para desarrolladores de Android antes de la entrada en vigor de la normativa en septiembre

Google anunció el lunes que comenzará a implementar oficialmente la verificación de desarrolladores de Android para todos los creadores, con el objetivo de combatir el problema de actores maliciosos que distribuyen aplicaciones dañinas mientras *“se ocultan tras el anonimato.”*

Este cambio se produce antes de un [requisito de verificación](#) que entrará en vigor este septiembre en Brasil, Indonesia, Singapur y Tailandia, y que posteriormente se ampliará a nivel global el próximo año.

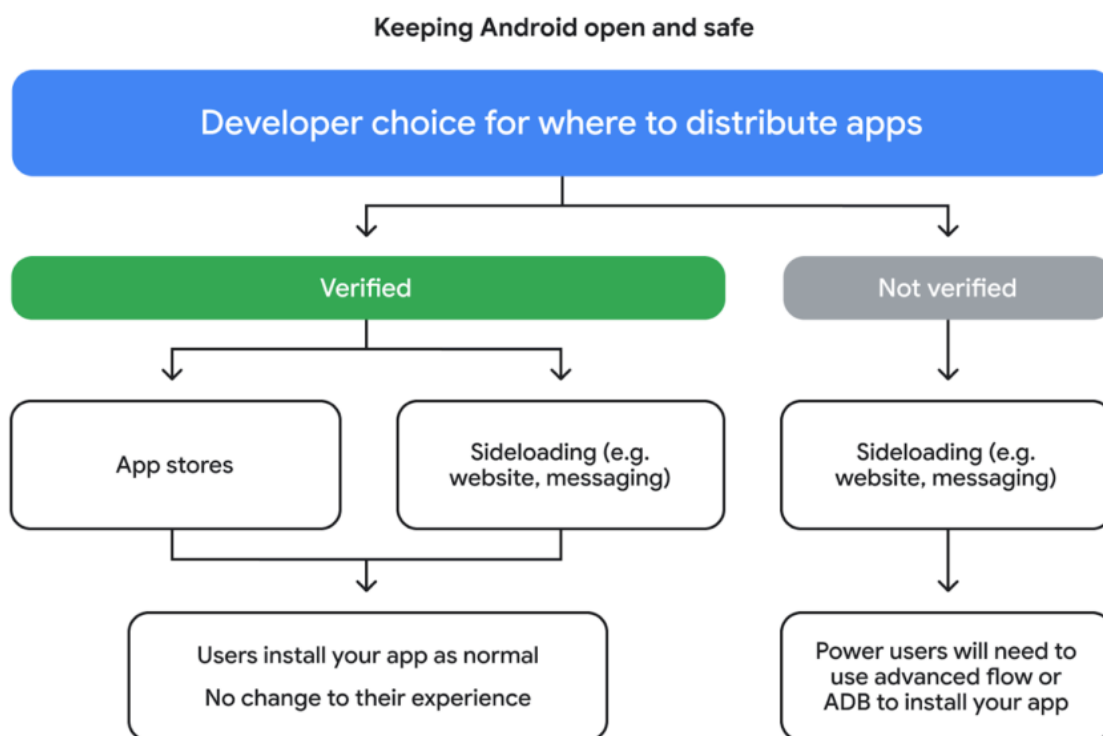
Como parte de esta iniciativa, Google exigirá que los desarrolladores que distribuyen aplicaciones fuera de Google Play creen una cuenta en la consola de desarrolladores de Android para confirmar su identidad. Aquellos que publican aplicaciones dentro del mercado oficial de Android y ya hayan verificado su identidad podrían estar *“ya preparados,”* según indicó la empresa tecnológica.

*“Para la gran mayoría de los usuarios, la experiencia de instalar aplicaciones seguirá siendo exactamente la misma,”* [explicó Matthew Forsythe](#), director de gestión de producto en Seguridad de Aplicaciones Android. *“Solo cuando un usuario intente instalar una app no registrada será necesario usar ADB o un flujo avanzado, lo que nos ayuda a mantener segura a la comunidad en general sin sacrificar la flexibilidad para los usuarios más avanzados.”*

Los desarrolladores que utilizan Android Studio podrán ver el estado de registro de sus aplicaciones directamente dentro del entorno de desarrollo integrado (IDE) en los próximos dos meses, al generar un App Bundle o APK firmado.



Ya comenzó el despliegue de verificación para desarrolladores de Android antes de la entrada en vigor de la normativa en septiembre



Aquellos desarrolladores que ya hayan completado los requisitos de verificación de Play Console verán cómo sus aplicaciones elegibles se registran automáticamente. En caso de que una app no pueda registrarse, se pedirá a los desarrolladores que sigan un proceso manual de reclamación.

Tal como se anunció hace unas semanas, los usuarios avanzados siempre tendrán la opción de habilitar la instalación manual (sideloading) de archivos APK no registrados mediante un flujo avanzado que incluye un paso de autenticación para confirmar que actúan por voluntad propia, además de un periodo de espera único de 24 horas para disuadir fraudes.

*“Este proceso es único para usuarios avanzados, pero ha sido diseñado cuidadosamente para evitar que quienes estén siendo objeto de una estafa sean presionados mediante tácticas*



Ya comenzó el despliegue de verificación para desarrolladores de Android antes de la entrada en vigor de la normativa en septiembre

*agresivas para instalar software malicioso,”* añadió Forsythe.

Este anuncio coincide con [cambios](#) realizados por Apple en su Acuerdo de Licencia del Programa de Desarrolladores, con el fin de reforzar las normas de privacidad relacionadas con el acceso de dispositivos wearables de terceros a actividades en vivo y notificaciones.

Apple indicó de forma explícita que los terceros *“no pueden utilizar la información reenviada para publicidad, creación de perfiles, entrenamiento de modelos ni para el seguimiento de la ubicación,”* y añadió que *“tampoco pueden compartir dicha información con ninguna otra aplicación ni con ningún dispositivo distinto del accesorio autorizado.”*

La nueva sección también subraya que los desarrolladores no pueden almacenar de forma remota esta información en servicios en la nube, realizar cambios que alteren *“de manera sustancial”* el significado del contenido, ni descifrar los datos en un lugar distinto al propio accesorio.