

Google Developer Policy - April 16, 2020

Queremos crear la fuente de apps y juegos más confiable del mundo

Su innovación impulsa nuestro éxito compartido, pero conlleva cierta responsabilidad. Las Políticas del Programa para Desarrolladores y el [Acuerdo de Distribución para Desarrolladores](#) nos permiten asegurarnos de seguir brindando juntos las aplicaciones más innovadoras y confiables del mundo a más de mil millones de personas a través de Google Play. Lo invitamos a explorar nuestras políticas a continuación o en la [vista de impresión](#).

Todos los días, personas de todo el mundo acceden a aplicaciones y juegos en Google Play. Antes de enviar una aplicación, debe asegurarse de que sea apropiada para Google Play y cumpla con las leyes locales.

Menores en situación de peligro

Las aplicaciones que incluyen contenido que sexualiza a menores de edad se eliminan inmediatamente de Store. No se permiten las aplicaciones atractivas para niños que incluyan temas de adultos.

Si se detecta contenido con imágenes de abuso sexual de menores, se notificará a las autoridades pertinentes y se borrarán las Cuentas de Google de todos los usuarios implicados en la distribución del contenido.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios. Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Contenido sexual

No se permiten aplicaciones que contengan o promuevan contenido sexual, como pornografía o cualquier otro tipo de contenido o servicio destinado a brindar placer de carácter sexual. Se permite la publicación de contenido que incluya desnudez si su objetivo principal es educativo, documental, científico o artístico, y no injustificado.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Representaciones de desnudez en las que el sujeto esté desnudo o vestido con poca ropa y cuyo atuendo no sea aceptable en un contexto público apropiado.

Representaciones, animaciones o ilustraciones de actos sexuales o posturas sexualmente provocativas.
Contenido que represente accesorios sexuales y fetiches.
Contenido lascivo o profano.
Contenido que represente, describa o promueva la zoofilia.
Aplicaciones que promuevan entretenimiento de tipo sexual, servicios de acompañantes o de otro tipo que puedan interpretarse como servicios que proporcionan actos sexuales a cambio de una compensación.

Incitación al odio o a la violencia

No permitimos aplicaciones que promuevan la violencia o fomenten el odio hacia una persona o hacia grupos de individuos en función de su origen étnico o raza, religión, discapacidad, edad, nacionalidad, condición de veterano de guerra, orientación sexual, género, identidad de género o alguna otra característica que esté asociada con la marginación o la discriminación sistémicas. Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Compilaciones de afirmaciones que pretendan probar que un grupo protegido es inhumano, inferior o que se lo debe odiar.

Aplicaciones que contengan teorías que indiquen que un grupo protegido posee características negativas (p. ej., que son malintencionados, corruptos, malvados, etc.) o afirmen de manera explícita o implícita que ese grupo es una amenaza.

Contenido o un discurso que pretenda alentar a otros a creer que se debe odiar o discriminar a las personas porque pertenecen a un grupo protegido.

Violencia

No permitimos aplicaciones que representen o muestren violencia gratuita u otras actividades peligrosas.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Representaciones gráficas o descripciones de violencia realista o amenazas violentas a personas o animales.

Aplicaciones que promuevan acciones como autolesiones, el suicidio, trastornos de alimentación, juegos de asfixia u otras que puedan provocar lesiones graves o la muerte.

Contenido relacionado con el terrorismo

No permitimos que las organizaciones terroristas publiquen aplicaciones en Google Play para ningún fin, incluido el reclutamiento.

No permitimos aplicaciones que incluyan contenido relacionado con el terrorismo, como el que fomente actos terroristas, incite a la violencia o celebre ataques terroristas. Si publicas contenido relacionado con el terrorismo para fines educativos, documentales, científicos o

artísticos, ten presente que debes brindar la información suficiente para que los usuarios entiendan el contexto.

Acontecimientos de carácter delicado

No permitimos aplicaciones que carezcan de sensibilidad razonable o que se aprovechen de los desastres naturales, las atrocidades, los conflictos, la muerte y otros acontecimientos trágicos. Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Demostrar falta de sensibilidad ante la muerte de una persona o un grupo de personas por motivos de suicidio, sobredosis, causas naturales y otros
- Negar un acontecimiento trágico de gran envergadura
- Obtener ganancias a costas de un acontecimiento trágico sin que se observe ningún beneficio para las víctimas

Hostigamiento y acoso

No permitimos aplicaciones que contengan o faciliten el bullying, el acoso o las amenazas. Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Hacer bullying a víctimas de conflictos religiosos o internacionales
- Intentar explotar a terceros con determinado contenido, incluidos los conceptos de chantaje y extorsión, entre otros
- Publicar contenido con el fin de humillar públicamente a alguien
- Hostigar a las víctimas de un acontecimiento trágico o sus amigos y familiares

Productos peligrosos

No permitimos aplicaciones que faciliten la venta de explosivos, armas de fuego, municiones o ciertos accesorios para armas.

Los accesorios restringidos son aquellos que permiten que un arma de fuego simule disparos automáticos o convierten un arma de fuego en una automática (p. ej., mecanismos de rebote, gatillos de repetición, accesorios que permiten transformar un arma en un rifle de asalto y kits de conversión), así como cargadores y estuches que transporten más de 30 cartuchos.

No permitimos aplicaciones que brinden instrucciones para la fabricación de explosivos, armas de fuego, municiones, accesorios para armas de fuego restringidos o cualquier otra arma. Esta restricción incluye las instrucciones para convertir un arma de fuego en una que dispare de manera automática o simule hacerlo.

Marihuana

No se permiten aplicaciones que faciliten la venta de marihuana ni productos de la marihuana, independientemente de su legalidad.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Permitir que las personas pidan marihuana mediante una función de carrito de compra en la aplicación

- Brindar asistencia a los usuarios para que organicen el retiro o la entrega de marihuana

- Facilitar la venta de productos que contengan THC

Tabaco y alcohol

No permitimos aplicaciones que faciliten la venta de tabaco (incluidos los cigarrillos electrónicos) o promuevan el uso irresponsable de alcohol o tabaco.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Representar o promover el uso o la venta de alcohol o tabaco a menores

- Insinuar que el consumo de tabaco puede mejorar la condición social, sexual, profesional o atlética

- Mostrar el consumo excesivo de alcohol como algo positivo, incluida la representación positiva del consumo excesivo, sostenido o competitivo

No se permiten aplicaciones que expongan a los usuarios a productos y servicios financieros engañosos o dañinos.

Para los efectos de esta política, se considera que los productos y servicios financieros son aquellos relacionados con la administración o la inversión de dinero y criptomonedas, incluido el asesoramiento personalizado.

Si una aplicación contiene o promueve productos y servicios financieros, debe cumplir con las reglamentaciones estatales y locales de todas las regiones o países a los que se oriente; por ejemplo, debe incluir las divulgaciones específicas que requiera la legislación local.

Opciones binarias

No se permiten aplicaciones que brinden a los usuarios la posibilidad de comercializar opciones binarias.

Criptomonedas

No se permiten aplicaciones que validen criptomonedas en los dispositivos. Permitimos las aplicaciones que administran la validación de criptomonedas de manera remota.

Préstamos personales

Definimos los préstamos personales como aquellos préstamos de dinero que un individuo, una organización o una entidad otorga a un consumidor individual de manera no recurrente y que no tienen como objetivo financiar la compra de un activo fijo ni educación. Los consumidores de préstamos personales requieren información sobre la calidad, las características, las tarifas, los

riesgos y los beneficios de los productos de préstamos para poder tomar decisiones fundamentadas en cuanto a solicitar o no el préstamo.

Ejemplos: préstamos personales, préstamos de nómina, préstamos entre pares, préstamos de título

Productos no incluidos: hipotecas, préstamos para la compra de vehículos, préstamos para estudiantes, líneas de crédito rotativo (como tarjetas de crédito, líneas de crédito personales)

Las aplicaciones de préstamos personales deben divulgar la siguiente información en los metadatos de la aplicación:

Período mínimo y máximo para el pago

Tasa anual efectiva (TAE) máxima, que por lo general incluye la tasa de interés más las tarifas y otros cargos por un año, o alguna otra tasa similar que se calcule en concordancia con la legislación local

Un ejemplo representativo del costo total del préstamo, incluidas todas las tarifas aplicables

No se permiten aplicaciones que promuevan préstamos personales que requieran el pago íntegro en 60 días o menos desde la fecha de emisión del préstamo (nos referimos a estos como "préstamos personales a corto plazo"). Esta política se aplica a las aplicaciones que ofrecen préstamos de forma directa, las que generan oportunidades de negocios y las que conectan a los consumidores con prestamistas externos.

Préstamos personales con TAE alto

En los Estados Unidos, no se permiten aplicaciones de préstamos personales en las que la tasa anual efectiva (TAE) sea del 36% o más alta. Las aplicaciones de préstamos personales publicadas en los Estados Unidos deben mostrar la TAE máxima, calculada en concordancia con la [Ley de Veracidad en Préstamos \(TILA\)](#).

Esta política se aplica a las aplicaciones que ofrecen préstamos de forma directa, las que generan oportunidades de negocios y las que conectan a los consumidores con prestamistas externos.

Juegos de apuestas

Se permiten servicios, contenido y anuncios que faciliten los juegos de apuestas en línea, siempre que cumplan con determinados requisitos. También se permiten aplicaciones de deportes de fantasía diarios que cumplan con ciertas especificaciones.

Aplicaciones de juegos de apuestas

(Actualmente se permiten solo en Francia, Irlanda y el Reino Unido)

El contenido y los servicios de juegos de apuestas en línea están permitidos siempre y cuando cumplan con los siguientes requisitos:

- El desarrollador debe [completar el proceso de solicitud](#) para poder distribuir la aplicación en Play.
- La aplicación debe cumplir con todas las leyes y los estándares de la industria aplicables en todos los países donde se distribuye.
- El programador debe tener una licencia de juegos de apuestas válida para cada país donde se distribuye la aplicación.
- La aplicación debe impedir que los usuarios menores de edad hagan apuestas dentro de ella.
- La aplicación debe impedir su uso en países que no estén incluidos en la licencia de juegos de apuestas proporcionada por el desarrollador.
- La aplicación NO debe poder comprarse como una aplicación pagada en Google Play ni usar la Facturación integrada en Google Play.
- La descarga y la instalación de la aplicación desde Play Store deben ser gratuitas.
- La aplicación debe estar clasificada como "Solo para adultos" (AO) o un equivalente de la IARC.
- La aplicación y su ficha deben mostrar información clara sobre el uso responsable de los juegos de apuestas.

Para todas las demás ubicaciones, no se permite contenido ni servicios de juegos de apuestas en línea, entre los que se incluyen, sin limitarse a ellos, casinos en línea, apuestas deportivas, loterías y juegos de habilidad que ofrezcan premios en efectivo o con otro valor en el mundo real.

Anuncios de juegos de apuestas en aplicaciones que se distribuyen en Google Play

Se permiten anuncios de juegos de apuestas en línea siempre y cuando cumplan con los siguientes requisitos:

- La aplicación y el anuncio (así como los anunciantes de juegos de apuestas) deben cumplir con todas las leyes y los estándares de la industria aplicables en todas las ubicaciones donde se muestre el anuncio de juegos de apuestas.
- El anuncio debe cumplir con los requisitos de licencias locales para todos los productos y servicios relacionados con juegos de apuestas que se promocionen.
- La aplicación no debe mostrar anuncios de juegos de apuestas a menores de 18 años.
- La aplicación no debe estar inscrita en el programa Designed for Families.
- La aplicación no debe estar orientada a menores de 18 años.
- El anuncio debe brindar información clara sobre el uso responsable de los juegos de apuestas en la página de destino, en la ficha de la aplicación anunciada o dentro de la aplicación.

La aplicación que muestre un anuncio de juegos de apuestas no debe ser una aplicación de simulación de juegos de apuestas (un juego de entretenimiento sin apuestas con dinero real).

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Aplicación de "KIDS 123" que contenga un anuncio donde se promocionen servicios de juegos de apuestas

Aplicaciones de deportes de fantasía diarios (DFS)

Permitimos aplicaciones de deportes de fantasía diarios (DFS) siempre que cumplan con los siguientes requisitos:

El acceso a la aplicación y su distribución deben estar limitados a Estados Unidos. Las aplicaciones de DFS orientadas a jurisdicciones fuera de EE.UU. deben calificar como aptas por medio del proceso para aplicaciones de juegos de apuestas con dinero real. El desarrollador debe completar correctamente el proceso de [solicitud de DFS](#) y recibir la aceptación para poder distribuir la aplicación en Play.

La aplicación debe cumplir con todas las leyes y los estándares de la industria aplicables en todos los estados o territorios de EE.UU. en los que se distribuya.

El desarrollador debe tener una licencia válida para cada uno de los estados o territorios de EE.UU. en los que se requiera una para las aplicaciones de deportes de fantasía diarios.

La aplicación debe impedir que los usuarios menores de edad hagan apuestas o realicen transacciones monetarias dentro de ella.

La aplicación debe impedir su uso en los estados o territorios de EE.UU. en los que el desarrollador no posea la licencia requerida para las aplicaciones de deportes de fantasía diarios.

La aplicación debe impedir su uso en los estados o territorios de EE.UU. donde las aplicaciones de deportes de fantasía diarios no sean legales.

La aplicación NO debe poder comprarse como una aplicación pagada en Google Play ni usar la Facturación integrada en Google Play.

La descarga y la instalación de la aplicación desde Play Store deben ser gratuitas.

La aplicación debe estar clasificada como "Solo para adultos" (AO) o un equivalente de la IARC.

La aplicación y su ficha deben mostrar información clara sobre el uso responsable de los juegos de apuestas.

No permitimos aplicaciones que faciliten o promuevan actividades ilegales.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Facilitar la compra o venta de drogas ilegales o medicamentos con prescripción sin receta

Representar o promover el uso o la venta de drogas, alcohol o tabaco a menores.
Instrucciones para el cultivo o fabricación de drogas ilegales

Contenido generado por usuarios

El contenido generado por usuarios (CGU) es aquel que estos aportan a una aplicación y que está visible o accesible para un subgrupo de usuarios de ella. El contenido inaceptable es aquel que incumple nuestras políticas.

Las aplicaciones que incluyan CGU deben cumplir con lo siguiente:

- requerir que los usuarios acepten las Condiciones de uso o políticas del usuario de la aplicación antes de que ellos creen o suban CGU
- definir el CGU que es inaceptable y prohibirlo por medio de sus Condiciones de uso o políticas del usuario de manera consistente con el espíritu de las Políticas del programa para desarrolladores de Google Play
- implementar la moderación del CGU de manera rigurosa, efectiva y continua, y de forma razonable y coherente con el(los) tipo(s) de CGU que aloja la aplicación
- brindar un sistema integrado en la aplicación y fácil de usar para denunciar y quitar el CGU inaceptable
 - En el caso de las aplicaciones de streaming en vivo, el CGU problemático debe quitarse prácticamente en tiempo real (tan pronto como sea razonablemente posible)
- quitar o bloquear a los usuarios con comportamiento inadecuado que infrinjan las condiciones de uso o la política del usuario de la aplicación
- proporcionar protecciones para evitar que la monetización dentro de la aplicación promueva un comportamiento reprochable por parte del usuario

Se quitarán de Google Play aquellas aplicaciones cuyo propósito principal sea mostrar CGU inaceptable. De manera similar, también se quitarán de Google Play las aplicaciones que se usen principalmente para alojar CGU reprochable o que adquieran la reputación de fomentar dicho contenido entre los usuarios.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Promoción de contenido sexual explícito generado por el usuario, incluida la implementación de funciones pagas cuyo principal objetivo sea fomentar que los usuarios compartan contenido reprochable.

Aplicaciones que incluyan contenido generado por usuarios (CGU), pero que no contengan suficiente protección contra amenazas, hostigamiento o acoso, en especial hacia menores.

Publicaciones, comentarios o fotos dentro de una aplicación cuyo objetivo principal sea acosar o someter a una persona al abuso, a ataques malintencionados o al ridículo.

Aplicaciones que de manera continua no resuelvan las denuncias de los usuarios acerca del contenido inaceptable.

Google Play no permite aplicaciones que promuevan ni vendan sustancias no aprobadas, independientemente de cualquier alegato de legalidad. Ejemplos:

Todos los artículos de esta lista no exhaustiva de [productos farmacéuticos y suplementos prohibidos](#)

Productos que contienen efedra

Productos que contienen gonadotropina coriónica humana (hCG) en relación con la pérdida o el control del peso, o si se promocionan junto con esteroides anabólicos

Suplementos herbales y dietéticos con ingredientes farmacéuticos activos o peligrosos

Declaraciones falsas o engañosas de beneficios terapéuticos, incluidas las afirmaciones que insinúen que un producto es tan eficaz como los medicamentos de venta con receta o las sustancias controladas

Productos sin aprobación gubernamental que se comercialicen de una manera que insinúe que su uso es seguro o que son eficaces para prevenir, curar o tratar determinadas enfermedades o problemas de salud

Productos que hayan estado sujetos a acciones o advertencias reguladoras o gubernamentales

Productos con nombres que pueden confundirse con productos farmacéuticos, sustancias controladas o suplementos no aprobados

Para obtener más información acerca de los productos farmacéuticos y suplementos no aprobados o engañosos que supervisamos, visita www.legitscript.com.

Robo de identidad y propiedad intelectual

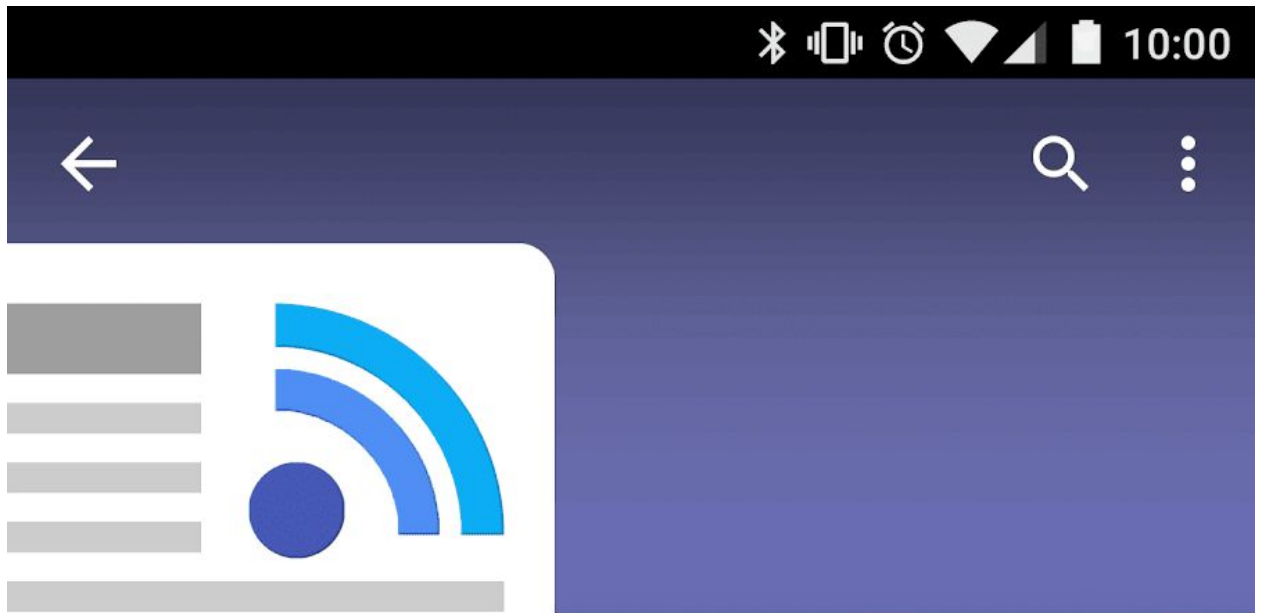
Cuando los desarrolladores copian el trabajo de otra persona o engañan a los usuarios, perjudican no solo a los usuarios, sino también a la comunidad de desarrolladores. No confíe en el uso engañoso o desleal del trabajo de otras personas.

Robo de identidad

No se permiten aplicaciones que usen marcas, títulos, logotipos o nombres de otras aplicaciones o entidades de forma tal que puedan engañar a los usuarios. No intente insinuar que existe algún tipo de vinculación o relación con otra entidad si no es cierto. El robo de identidad puede ocurrir incluso si no existe la intención de engañar. Por eso, tenga cuidado cuando se refiera a otras marcas que no le pertenecen. Este aspecto se aplica incluso si la marca aún no se encuentra en Google Play.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Desarrolladores que sugieren una falsa afiliación con otra entidad:



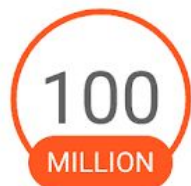
1

RSS News Aggregator

Google Developer

E Everyone

INSTALL



Downloads



161,251 



News &
Magazines



Similar

All the best news, aggregated in one spot!



WHAT'S NEW

- Push notifications now enabled.

- Customize your feed based on your current location!

① El nombre del programador para esta aplicación sugiere una relación oficial con Google, aunque no existe dicha relación.

Los íconos y títulos de aplicaciones que son tan parecidos a los de otros productos o servicios existentes que pueden confundir a los usuarios:

	 Google Maps	 Google+	 YouTube	 Twitter
	 Google Maps Navigator	 Google+ Sharify	 YouTube Aggregator	 TwitterPro

aplicaciones que falsamente afirman ser la aplicación oficial de una entidad establecida. No se permite usar títulos como "Oficial de Justin Bieber" sin los permisos o derechos necesarios.

Aplicaciones que infringen los [Lineamientos de marca de Android](#).

Propiedad intelectual

No permitimos aplicaciones ni cuentas de desarrolladores que infrinjan los derechos de propiedad intelectual de terceros (marcas registradas, derechos de autor, patentes, secretos comerciales y otros derechos de propiedad). Tampoco admitimos aplicaciones que fomenten o motiven el incumplimiento de los derechos de propiedad intelectual.

Responderemos a las notificaciones claras sobre presuntos incumplimientos de los derechos de autor. Para obtener más información o enviar una solicitud de DMCA, consulta nuestros [procedimientos relacionados con los derechos de autor](#).

Para enviar un reclamo sobre la venta o promoción para la venta de productos falsificados dentro de una aplicación, envía un [aviso de falsificación](#).

Si eres propietario de una marca comercial y crees que hay una aplicación en Google Play que infringe los derechos de tu marca, comunícate directamente con el desarrollador para resolver el problema directamente. Si no puede llegar a un acuerdo con el desarrollador, envíe un reclamo por uso de marca mediante este [formulario](#).

Si cuenta con documentación escrita que demuestre que tiene permiso para usar la propiedad intelectual de un tercero en su aplicación o ficha de Play Store (como nombres de marcas, logotipos y recursos gráficos), [comuníquese con el equipo de Google Play](#) antes de realizar el

envío para asegurarse de que no se rechace la aplicación debido a un incumplimiento de la propiedad intelectual.

Uso no autorizado del contenido protegido por derechos de autor

No permitimos aplicaciones que incumplan los derechos de autor. La modificación de contenidos protegidos por derechos de autor puede derivar en incumplimiento de la política. Es posible que se solicite a los desarrolladores que demuestren la posesión de derechos para usar el contenido protegido por derechos de autor.

Ten cuidado cuando uses contenido protegido por derechos de autor para demostrar la funcionalidad de tu aplicación. En general, el enfoque más seguro es crear algo que sea original.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Material gráfico para álbumes de música, videojuegos y libros

- Imágenes de comercialización de películas, televisión o videojuegos.

- Material gráfico o imágenes de libros de cómics, dibujos animados, películas, videos de música o televisión.

- Logotipos de equipos deportivos profesionales y universitarios.

- Fotos tomadas de la cuenta de medios sociales de una persona pública.

- Imágenes profesionales de personas públicas.

- Reproducciones o "fan art" que no puedan distinguirse de la obra original protegida por derechos de autor.

- aplicaciones que tienen consolas que reproducen clips de audio de contenido protegido por derechos de autor.

- Reproducciones completas o traducciones de libros que no son de dominio público

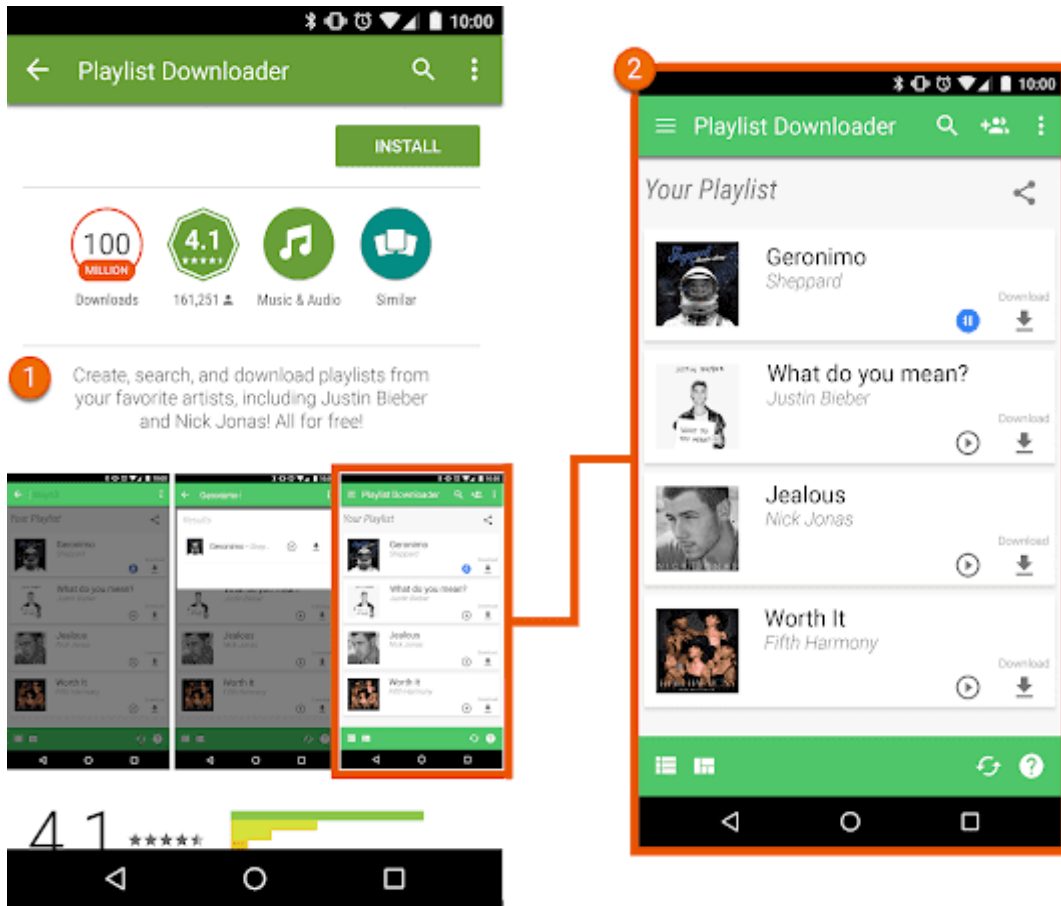
Acciones que fomentan el incumplimiento de los derechos de autor

No permitimos aplicaciones que induzcan o fomenten el incumplimiento de los derechos de autor. Antes de publicar la aplicación, busca posibles formas en las que esta pueda fomentar el incumplimiento de los derechos de autor y pide asesoramiento legal (si fuera necesario).

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Apps de streaming que permitan que los usuarios descarguen copias locales de contenido protegido por derechos de autor sin autorización

- Aplicaciones que induzcan a los usuarios a transmitir y descargar obras protegidas por derechos de autor, incluido el contenido de música y video, que infringe la legislación vigente sobre derechos de autor:



- ① La descripción en la ficha de la app alienta a los usuarios a descargar contenido protegido por derechos de autor sin autorización.
- ② La captura de pantalla de la ficha de la app alienta a los usuarios a descargar contenido protegido por derechos de autor sin autorización.

Infracción de marca registrada

No permitimos aplicaciones que infrinjan marcas registradas de terceros. Una marca comercial es una palabra, un símbolo o una combinación de ambos que identifica el origen de un producto o servicio. Una vez que se adquiere, la marca comercial le otorga al propietario derechos exclusivos para el uso de la marca con respecto a determinados productos y servicios.

La infracción de marcas comerciales supone un uso inadecuado o no autorizado de una marca comercial idéntica o similar, de tal forma que es posible que provoque confusión con respecto al origen de ese producto. Si tu aplicación usa una marca registrada de un tercero de tal forma que sea probable que provoque confusión, es posible que se suspenda.

Falsificación

No permitimos aplicaciones que vendan o promuevan la venta de productos falsificados. Los productos falsificados son aquellos que contienen una marca comercial o un logotipo que es igual a la marca comercial de otro producto, o bien que es prácticamente imposible de diferenciar. Dichos productos imitan las características de marca del producto para aparentar ser un producto auténtico del propietario de la marca.

Privacidad, seguridad y engaño

Nos comprometemos a proteger la privacidad del usuario y a brindarle un entorno seguro. Se prohíben estrictamente las aplicaciones engañosas, malintencionadas o que abusen o hagan uso inadecuado de cualquier red, dispositivo o dato personal.

Datos del usuario

Debes ser honesto en lo que respecta a la forma de manejar los datos del usuario (p. ej., la información que proporciona un usuario y la que se recopila sobre él, incluida la relacionada con dispositivos). Es decir, debe divulgar si su aplicación accede a los datos, así como cuándo los recopila, usa y comparte, además de limitar su uso a los fines divulgados. Por otra parte, si la aplicación administra datos personales o sensibles del usuario, consulta los requisitos adicionales en la sección "Información Personal y Sensible" más abajo. Estos requisitos de Google Play se agregan a las condiciones prescritas por las leyes aplicables en materia de privacidad y protección de los datos.

Información Personal y Sensible

Los datos sensibles y personales de los usuarios incluyen, sin limitarse a ello, información de identificación personal, financiera, de pago y de autenticación; datos relacionados con la agenda telefónica, contactos, [ubicación del dispositivo](#), SMS y llamadas; información del micrófono y la cámara, y otros datos sensibles relacionados con el uso o el dispositivo. Si tu aplicación administra datos sensibles de los usuarios, debes realizar lo siguiente:

Limita su acceso a los datos personales o sensibles adquiridos a través de la aplicación, así como la recopilación, el uso y el uso compartido de esa información, para fines directamente relacionados con la provisión y mejora de las funciones de la aplicación (p. ej., una función que espera el usuario y que se documenta y anuncia en su descripción en Play Store). Las aplicaciones que extienden el uso de estos datos para publicar anuncios deben cumplir con nuestra [Política de Anuncios](#).

Publica una política de privacidad, tanto en el campo designado en Play Console como en la aplicación. La política de privacidad, junto con cualquier otro aviso de divulgación integrado en la aplicación, debe explicar detalladamente cómo la aplicación accede a los datos del usuario, además de cómo los recopila, usa y comparte. Tu política de privacidad debe revelar los tipos de datos personales y sensibles que recopila, usa y

comparte la aplicación, y a los que tiene acceso, así como los tipos de terceros con los que se comparten datos personales o sensibles de los usuarios.

Administra todos los datos personales o confidenciales de los usuarios de forma segura, lo que incluye transmitirlos mediante con criptografía moderna (por ejemplo, por HTTPS).

Cuando esté disponible, usa una solicitud de permisos de tiempo de ejecución antes de acceder a los datos mediante [permisos de Android](#).

No vendas los datos sensibles ni personales de los usuarios.

Divulgación destacada y requisito de consentimiento

Según lo determine Play a su total discreción, en los casos en que tal vez los usuarios no tengan una expectativa razonable de que sus datos personales o sensibles sean necesarios para proporcionar o mejorar las características o las funciones que cumplan con las políticas dentro de su aplicación, deberás cumplir con los siguientes requisitos:

Debes proporcionar una divulgación integrada en la aplicación sobre el acceso, la recopilación y el uso de los datos, así como con quién se comparten. La divulgación debe cumplir con lo siguiente:

- Debe estar dentro de la app, no solo en su descripción o en un sitio web.

- Se debe mostrar durante el uso normal de la app sin que el usuario tenga que ir al menú o la configuración.

- Debe describir los datos a los que se accede o que se recopilan.

- Debe explicar cómo se usarán o compartirán los datos.

- No se puede colocar únicamente en la política de privacidad o en las condiciones del servicio.

- No se puede incluir con otras divulgaciones que no estén relacionadas con la recopilación de datos personales o sensibles.

La divulgación integrada en la aplicación debe ir acompañada de una solicitud de consentimiento del usuario inmediatamente posterior y, cuando esté disponible, un permiso de tiempo de ejecución asociado. No podrás acceder a datos personales o sensibles, ni recopilarlos, hasta que el usuario otorgue su consentimiento. La solicitud de consentimiento de la aplicación debe cumplir con lo siguiente:

- Debe presentar el diálogo de consentimiento de manera clara y sin ambigüedades.

- Debe exigir acciones afirmativas del usuario (p. ej., presionar para aceptar o marcar una casilla).

- No debe interpretar como consentimiento la acción de salir de la divulgación (incluidos presionar para salir o presionar el botón de inicio o atrás).

- No debe usar mensajes que caduquen o se descarten automáticamente.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Una aplicación que accede al inventario de aplicaciones instaladas de un usuario y no considera estos datos como personales o sensibles de acuerdo con los requisitos de Transmisión Segura, Divulgación Clara y la Política de Privacidad

Una aplicación que accede a los datos del teléfono o los contactos de un usuario y no considera estos datos como personales o sensibles de acuerdo con los requisitos de Transmisión Segura, Divulgación Clara y la Política de Privacidad

Una aplicación que graba la pantalla del usuario y no trata esta información como datos personales o sensibles sujetos a esta política

Una aplicación que recopila la **ubicación del dispositivo** y no divulga su uso de manera exhaustiva de acuerdo con los requisitos anteriores

Restricciones sobre el acceso a datos sensibles

Además de los requisitos anteriores, la siguiente tabla describe los requisitos para actividades específicas.

Actividad	Requisito
Tu aplicación administra información financiera o de pago, o bien números de identificación nacional	Su aplicación nunca debe divulgar públicamente datos personales ni confidenciales de los usuarios relacionados con actividades financieras o de pago, ni números de identificación nacional.
Tu aplicación administra información de contacto o de agendas telefónicas no públicas	No permitimos la divulgación ni la publicación de los contactos no públicos de los usuarios.
Tu aplicación contiene funciones de seguridad o de control de virus, como antivirus, eliminación de software malicioso o alguna otra función relacionada con la seguridad	Tu aplicación debe publicar una política de privacidad que, junto con cualquier otro aviso de divulgación integrado, explique detalladamente qué datos del usuario se recopilan y transmiten, cómo se usan y con quién se comparten.

EU-U.S. Privacy Shield (Escudo de Privacidad UE-EE.UU.)

Si procesas o usas información personal compartida por Google o accedes a datos que identifiquen de forma directa o indirecta a algún individuo cuya información se originó en la Unión Europea o Suiza ("Información Personal de la UE"), ten en cuenta lo siguiente:

Debes cumplir con todas las leyes, directivas, regulaciones y reglas de privacidad, protección y seguridad de los datos aplicables.

Debe procesar o usar la Información Personal de la UE, o acceder a estos datos, únicamente para fines acordes con el consentimiento otorgado por el individuo al cual se refiere dicha información.

Debes implementar medidas organizativas y técnicas apropiadas para proteger la Información Personal de la UE contra cualquier pérdida, uso inadecuado y acceso, divulgación, alteración o destrucción no autorizada o ilícita.

Debes proporcionar el mismo nivel de protección que requieren los [Principios de Privacy Shield \(Escudo de Privacidad\)](#).

Debes supervisar con frecuencia que cumples con estas condiciones. Si en algún momento no puedes cumplir con estas condiciones (o si existe un riesgo significativo de que no puedas cumplir con ellas), debes notificárnoslo de inmediato por correo electrónico a data-protection-office@google.com y dejar de procesar Información Personal de la UE o tomar las medidas razonables y adecuadas para restablecer un nivel de protección adecuado de inmediato.

Permisos

Los usuarios deben comprender las solicitudes de permisos. Solo puede solicitar permisos que sean necesarios para implementar funciones o servicios existentes en su aplicación que se promuevan en la ficha de Play Store. Se prohíbe el uso de permisos que concedan acceso a los datos del usuario o del dispositivo para funciones o fines no divulgados, no implementados o no autorizados. No se permite la venta de datos sensibles o personales a los que se acceda mediante permisos.

Solicite permisos para acceder a los datos en contexto (mediante la autenticación incremental), de modo que los usuarios comprendan por qué su aplicación los necesita. Use los datos solo para los fines para los que el usuario haya otorgado consentimiento. Si más adelante desea usar los datos para otros fines, debe solicitar el permiso de los usuarios y asegurarse de que acepten los propósitos adicionales.

Permisos Restringidos

Además de lo anterior, los permisos restringidos son aquellos que se designan como [de Firma](#) o [Riesgosos](#) en nuestra documentación para desarrolladores, y están sujetos a los requisitos y las restricciones adicionales que se indican a continuación:

Los datos sensibles de los dispositivos o los usuarios a los que se acceda mediante Permisos Restringidos solo se pueden transferir a terceros si son necesarios para proporcionar o mejorar funciones o servicios existentes en la aplicación que recopiló esos datos. También puede transferir datos cuando sea necesario para cumplir con la legislación aplicable o como parte de una fusión, adquisición o venta de activos, habiendo proporcionado una notificación legal adecuada a los usuarios. Se prohíben todas las demás transferencias o ventas de los datos de los usuarios. Se debe respetar la decisión de los usuarios si rechazan una solicitud de Permisos Restringidos; no se debe manipular ni forzar a los usuarios para que den su consentimiento a cualquier permiso que no sea crítico. Se deben realizar todos los

esfuerzos razonables para ajustar el contenido a los usuarios que no otorguen acceso a permisos sensibles (p. ej., permitir que un usuario ingrese un número de teléfono de forma manual si restringió el acceso a los Registros de Llamadas).

Algunos Permisos Restringidos pueden estar sujetos a los requisitos adicionales que se detallan a continuación. El objetivo de estas restricciones es proteger la privacidad de los usuarios. Es posible que hagamos excepciones limitadas a los requisitos en casos muy infrecuentes en los que las aplicaciones proporcionen una función crítica o sumamente atractiva para la que no exista un método alternativo disponible. Evaluaremos las excepciones propuestas en función de su impacto potencial sobre la privacidad o seguridad de los usuarios.

Permisos de SMS y Registro de Llamadas

Los Permisos de SMS y Registro de Llamadas se consideran datos sensibles y personales de los usuarios y están sujetos a la política de [Información Personal y Sensible](#), así como a las siguientes restricciones:

Permiso Restringido	Requisito
Grupo de permisos de Registro de Llamadas (p. ej., READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Debe estar registrado activamente como el controlador predeterminado de Teléfono o Asistente en el dispositivo.
Grupo de permisos de SMS (p. ej., READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Debe estar registrado activamente como controlador predeterminado de SMS o del Asistente en el dispositivo.

Las aplicaciones que no posean la función de controlador predeterminado del Asistente, Teléfono o SMS no pueden declarar el uso de los permisos anteriores en el manifiesto. Esto también se aplica al texto de marcador de posición en el manifiesto. Además, las aplicaciones deben estar registradas de forma activa como controladores predeterminados del Asistente, Teléfono o SMS antes de solicitar a los usuarios que acepten cualquiera de los permisos anteriores. Asimismo, deben finalizar de inmediato el uso del permiso cuando dejen de ser controladores predeterminados. En [esta página del Centro de ayuda](#), se pueden consultar los usos permitidos y las excepciones.

Las aplicaciones solo pueden usar el permiso (y cualquier dato derivado de este) para brindar la funcionalidad principal aprobada de la aplicación. La funcionalidad principal se define como el objetivo más importante de la aplicación. Esto puede incluir una serie de funciones principales, las cuales deben estar claramente documentadas y promocionadas en la descripción de la aplicación. Sin las funciones principales, la aplicación se considera "dañada" o inútil. Solo se deben transferir, compartir o usar con licencia estos datos a fin de brindar funciones o servicios principales dentro de la aplicación, y no se puede extender su uso para ningún otro propósito (p. ej., mejorar otras aplicaciones o servicios, publicidad o marketing). No se pueden usar métodos

alternativos (incluidos otros permisos, API o fuentes de terceros) para obtener datos atribuidos a los permisos de Registro de Llamadas o SMS relacionados.

Permisos de Ubicación

Actualización del 16 de abril de 2020: Sabemos que, a fin de cumplir con la política de Ubicación, algunos desarrolladores deberán ejercer un esfuerzo sustancial, por lo que ofrecemos un cronograma extendido para que puedan realizar todos los cambios necesarios. Para ver los cronogramas y otras actualizaciones, visita nuestro [Centro de ayuda](#).

Se considera que la [ubicación del dispositivo](#) es un dato sensible y personal del usuario, y está sujeto a la política de [Información Personal y Sensible](#), así como a los siguientes requisitos:

Las aplicaciones no pueden acceder a los datos protegidos por permisos de ubicación (p. ej., ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) luego de que estos dejen de ser necesarios para implementar funciones o servicios existentes dentro de la aplicación.

Nunca debes solicitar permisos de ubicación a los usuarios únicamente con fines de publicidad o análisis. Las aplicaciones que extienden el uso permitido de este dato para publicar anuncios deben cumplir con nuestra [Política de Anuncios](#).

Las aplicaciones deben solicitar el alcance mínimo necesario (es decir, ubicación aproximada en lugar de precisa y uso en primer plano en vez de en segundo plano) para proporcionar el servicio o la función en curso que requiere la ubicación, y los usuarios deben tener una expectativa razonable de que el servicio o la función necesita el nivel de ubicación solicitado. Por ejemplo, es posible que rechacemos las aplicaciones que soliciten acceso o que accedan a la ubicación en segundo plano sin una justificación convincente.

La ubicación en segundo plano solo se puede usar con el fin de proporcionar funciones beneficiosas para el usuario y relevantes para la funcionalidad principal de la aplicación.

Se permite que las aplicaciones accedan a la ubicación con un servicio en primer plano (cuando la aplicación solo tiene acceso en primer plano, p. ej., "durante el uso") si el uso cumple con las siguientes condiciones:

Se inició como una continuación de una acción iniciada por el usuario dentro de la aplicación.

Finaliza inmediatamente después de que la aplicación completa el caso práctico previsto de la acción iniciada por el usuario.

Las aplicaciones diseñadas específicamente para niños deben cumplir con la política de [Designed for Families](#).

Abuso de redes y dispositivos

No se permiten aplicaciones que interfieran con el dispositivo, lo interrumpan, lo dañen o accedan a él sin autorización, como tampoco a otros dispositivos ni computadoras, servidores, redes, interfaces de programación de aplicaciones (API) o servicios (incluidos, entre otros, a otras aplicaciones del dispositivo, cualquier servicio de Google o red de proveedor autorizada).

Las aplicaciones que se publiquen en Google Play deben cumplir con los requisitos de optimización del sistema Android predeterminado documentados en los [lineamientos de calidad de las aplicaciones en Google Play](#).

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Aplicaciones que bloquean o interfieren con otra app debido a la exhibición de anuncios

- Aplicaciones de trucos de juegos que afectan el juego en otras aplicaciones.

- Aplicaciones que facilitan o proporcionan instrucciones sobre cómo piratear servicios, software, hardware o cómo evadir las protecciones de seguridad.

- Aplicaciones que acceden o usan un servicio o una API de forma tal que incumplan las Condiciones del Servicio

- Aplicaciones que intentan acceder a la [administración de energía del sistema](#) y que no son [aptas para incluirlas en la lista blanca](#)

- Aplicaciones que facilitan servicios de proxy a terceros (solo deben hacerlo las aplicaciones que tengan esa finalidad como principal para el usuario)

Comportamiento malicioso

No se permiten aplicaciones que roben datos, monitoreen en secreto o dañen a los usuarios, o que sean de algún modo maliciosas.

Las aplicaciones que se distribuyan en Google Play no podrán modificarse, reemplazarse ni actualizarse con ningún otro método que no sea el mecanismo de actualización de Google Play. Tampoco se permite que las aplicaciones descarguen código ejecutable (p. ej., archivos dex, JAR o .so) de fuentes distintas a Google Play. Esta restricción no se aplica al código que se ejecuta en una máquina virtual y que tiene acceso limitado a las API de Android (como JavaScript en WebView o un navegador).

Solo se pueden descargar recursos adicionales de la aplicación (p. ej., recursos para juegos) si son necesarios para que el usuario pueda utilizar la aplicación. Los recursos que se descarguen deben cumplir con todas las políticas de Google Play y, antes de que comience la descarga, la aplicación deberá guiar a los usuarios e indicar claramente el tamaño de la descarga.

Se prohíbe explícitamente la publicación de aplicaciones de Vigilancia y Software Espía en Google Play. Solo las aplicaciones que cumplen con las políticas y que se diseñan y comercializan exclusivamente para el monitoreo parental (y familiar) o la administración empresarial pueden distribuirse en Play Store con funciones de informes y seguimiento, siempre y cuando cumplan con todos los requisitos que se describen a continuación.

Se prohíbe explícitamente lo siguiente:

Virus, troyanos, software maliciosos, software espía o cualquier otro tipo de software malicioso.

Aplicaciones que facilitan o se vinculan a la distribución o instalación de software malicioso

Aplicaciones o SDK que descargan código ejecutable, como archivos dex o código nativo, de una fuente que no sea Google Play

Aplicaciones que introducen o abusan de las vulnerabilidades de seguridad

Aplicaciones que roban la información de autenticación de un usuario (como nombres de usuario o contraseñas) o que se hacen pasar por otras aplicaciones o sitios web para que se revele información personal o de autenticación

Las aplicaciones no deben mostrar números de teléfono, contactos ni información de identificación personal sin verificar o reales de personas o entidades que no hayan brindado su consentimiento para ello

Aplicaciones que instalan otras aplicaciones en un dispositivo sin el previo consentimiento del usuario

Aplicaciones con descargas facilitadas por la red de distribución de contenidos (CDN) que no guían al usuario ni indican el tamaño de la descarga antes de que se inicie el proceso

Aplicaciones diseñadas para recopilar datos de uso del dispositivo en secreto, como las aplicaciones comerciales de software espía

Las aplicaciones que realizan un seguimiento del comportamiento de un usuario en un dispositivo o lo monitorean deben cumplir con lo siguiente:

Las aplicaciones no deben presentarse como una solución de espionaje o vigilancia secreta.

Las aplicaciones no deben ocultar ni encubrir el seguimiento del comportamiento, ni intentar engañar a los usuarios sobre esa función.

Se debe presentar ante los usuarios con una notificación persistente y un ícono único que identifique claramente a la aplicación.

Las aplicaciones y fichas que se muestran en Google Play no deben proporcionar ningún medio para activar o acceder a funcionalidades que infrinjan estos términos y condiciones, como vínculos a archivos APK alojados fuera de Google Play que no cumplan con dichos términos.

La responsabilidad de determinar la legalidad de la aplicación en el mercado de destino recae exclusivamente sobre ti. Las aplicaciones que se consideren ilegales en los lugares donde se hayan publicado se quitarán de los territorios respectivos.

Para obtener información sobre los problemas de seguridad más recientes que se informaron a los desarrolladores en Google Play, consulta nuestro [Programa de Mejora de la Seguridad de las Aplicaciones](#). Puedes encontrar más detalles sobre la vulnerabilidad y las soluciones en el vínculo de la página de ayuda de cada campaña.

Comportamiento engañoso

No se permiten aplicaciones que intenten engañar a los usuarios ni que den lugar a comportamientos deshonestos, lo que incluye, entre otras, aquellas diseñadas para ser funcionalmente imposibles. Las aplicaciones deben brindar información, descripciones videos o imágenes precisos de sus funciones en la totalidad de metadatos y deben funcionar dentro de las expectativas razonables del usuario. Las aplicaciones no deben intentar imitar las funciones ni las advertencias del sistema operativo ni de otras aplicaciones. Cualquier modificación en la configuración del dispositivo debe realizarse con el conocimiento y consentimiento del usuario, y este debe poder revertirla fácilmente.

Afirmaciones Engañosas

No se permiten aplicaciones que contengan información o afirmaciones falsas o engañosas en la descripción, el título, el ícono o la captura de pantalla.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Aplicaciones que tergiversen o no describan de forma precisa y clara su funcionalidad:

Una aplicación que afirma ser un juego de carreras en la descripción y en las capturas de pantalla, pero que en realidad es un juego de estrategia que usa la imagen de un automóvil

Una aplicación que afirma ser un antivirus, pero solo tiene texto que explica cómo quitar virus.

Nombres de aplicaciones o desarrolladores que tergiversen su estado o rendimiento actual en Google Play (p. ej., "Selección del editor", "App número 1", "Top ventas")

Aplicaciones que incluyan funciones o contenido médicos o relacionados con la salud que sean engañosos o potencialmente perjudiciales

Aplicaciones que afirmen tener funciones que no se puedan implementar

Aplicaciones que estén categorizadas de forma incorrecta

Contenido engañoso comprobable que pueda interferir con los procesos de votación

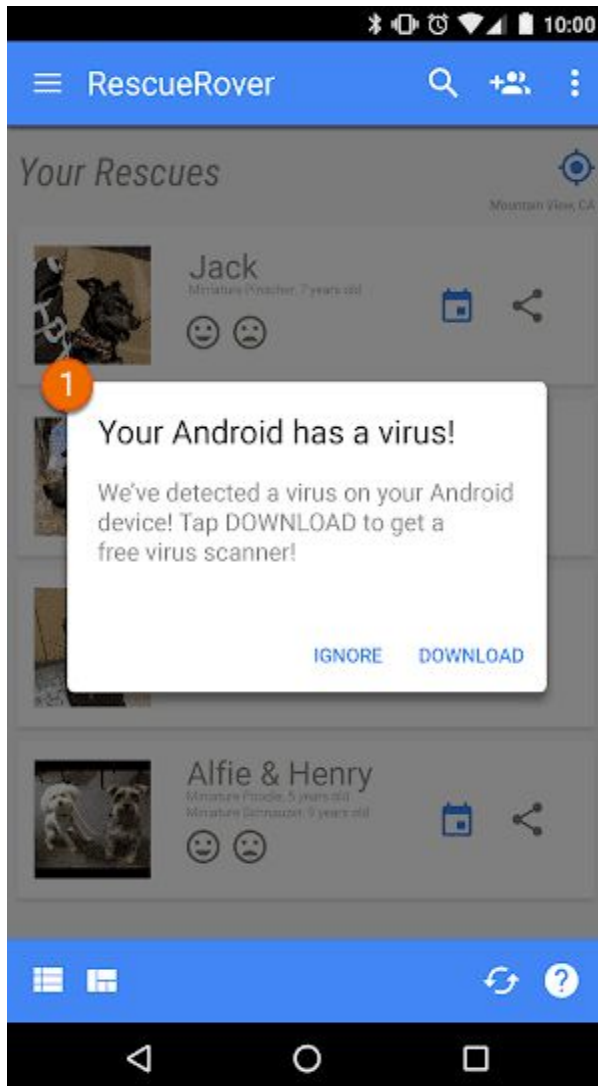
Aplicaciones que afirmen falsamente mantener algún vínculo con una entidad gubernamental o proporcionar o facilitar servicios gubernamentales para los cuales no están debidamente autorizadas

Uso No Autorizado o Imitación de las Funciones del Sistema

No se permiten aplicaciones o anuncios que imiten las funciones del sistema o interfieran con ellas, como las notificaciones o advertencias. Las notificaciones a nivel del sistema solo pueden usarse para funciones integrales de una aplicación, por ejemplo, la de una aerolínea que notifica a los usuarios sobre ofertas especiales o un juego que informa acerca de las promociones que se incluyen en él.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Aplicaciones y anuncios que se envían por medio de una notificación o alerta del sistema:



① La notificación del sistema que se muestra en esta aplicación se usa para publicar un anuncio.

Para ver ejemplos adicionales que incluyan anuncios, consulta la [política de Anuncios](#).

Cambios Engañosos en la Configuración del Dispositivo

No se permiten aplicaciones que modifiquen la configuración o las funciones del dispositivo del usuario fuera de la aplicación sin el conocimiento y consentimiento del usuario. Las funciones y la configuración del dispositivo incluyen la configuración del sistema y el navegador, los marcadores, las combinaciones de teclas, los íconos, los widgets y la presentación de las aplicaciones en la pantalla principal.

Tampoco permitimos lo siguiente:

- aplicaciones que modifican la configuración o las funciones con el consentimiento del usuario, pero lo hacen de forma tal que no es sencillo revertir la acción.
- aplicaciones o anuncios que modifican la configuración o las funciones del dispositivo como un servicio a terceros o con fines publicitarios.
- aplicaciones que engañan a los usuarios para que quiten o inhabiliten aplicaciones de terceros, o modifiquen la configuración o las funciones del dispositivo.
- Aplicaciones que fomentan o incentivan a los usuarios a que quiten o inhabiliten apps de terceros, o modifiquen la configuración o las funciones del dispositivo, a menos que sean parte de un servicio de seguridad comprobable

Prácticas que Fomentan un Comportamiento Fraudulento

No se permiten aplicaciones que faciliten que los usuarios engañen a otros ni que sean funcionalmente engañosas, lo que incluye, entre otras, aplicaciones que generen o faciliten la creación de tarjetas de identificación, números de seguridad social, pasaportes, diplomas, tarjetas de crédito y licencias de conducir. Las aplicaciones deben brindar información, títulos, descripciones, imágenes y videos precisos respecto de las funciones o el contenido que ofrecen, y funcionar de manera razonable y correcta tal como lo espera el usuario.

Las declaraciones que afirmen que una app es una "broma" o que "tiene fines de entretenimiento" (o cualquier otro sinónimo) no la eximen de cumplir con nuestras políticas.

Manipulación de Contenido Multimedia

No se permiten aplicaciones que promuevan o ayuden a crear información falsa o engañosa, ni afirmaciones transmitidas a través de imágenes, videos o texto. No se permiten aplicaciones diseñadas para promover o perpetuar imágenes, videos o textos engañosos comprobables, que puedan provocar daños con relación a un acontecimiento de carácter sensible, política, problemas sociales y otros asuntos de interés público.

Las aplicaciones que manipulan o alteran contenido multimedia más allá de los ajustes convencionales y editorialmente aceptables por motivos de claridad o calidad deben divulgar esta información de manera visible o colocar una marca de agua en el contenido multimedia alterado cuando, para la persona promedio, pueda no ser claro que el contenido multimedia se alteró. Se pueden otorgar excepciones para asuntos de interés público, sátiras o parodias evidentes.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Aplicaciones que agregan una figura pública a una protesta durante un evento políticamente sensible

Aplicaciones que usan figuras públicas o contenido multimedia a partir de un evento sensible para publicitar contenido multimedia que altera la capacidad dentro de la ficha de Play Store de una aplicación

Aplicaciones que alteran clips con contenido multimedia para imitar transmisiones de noticias

Tergiversación

Se prohíbe el uso de aplicaciones o cuentas de desarrolladores que roben la identidad de una organización o persona, o que oculten o tergiversen su propietario o su finalidad principal. No permitimos aplicaciones ni cuentas de desarrolladores que participen en actividades coordinadas para engañar a los usuarios, por ejemplo, pero sin limitarse a ello, las que ocultan o tergiversan su país de origen y dirigen su contenido a usuarios de otro país.

Software malicioso

Nuestra política de Software Malicioso es simple: el ecosistema de Android, incluido Google Play Store, y los dispositivos de los usuarios deben estar libres de comportamientos maliciosos (es decir, software malicioso). A través de este principio fundamental, nos esforzamos por ofrecer un ecosistema de Android seguro para nuestros usuarios y sus dispositivos Android.

Software malicioso es cualquier código que pudiera poner en riesgo a un usuario, sus datos o un dispositivo. El software malicioso incluye, entre otras cosas, aplicaciones potencialmente dañinas (APD), objetos binarios o modificaciones del marco de trabajo, e incluye categorías como troyanos, suplantación de identidad (phishing) y aplicaciones de software espía, que se actualizan permanentemente a la vez que se agregan otras nuevas.

Si bien varía en cuanto al tipo y las capacidades, el software malicioso suele tener uno de los siguientes objetivos:

- Comprometer la integridad del dispositivo del usuario
- Obtener control sobre el dispositivo de un usuario
- Habilitar operaciones controladas de manera remota para que el atacante pueda acceder al dispositivo infectado, usarlo o abusar de él de otro modo
- Transmitir datos personales o credenciales fuera del dispositivo sin la notificación y el consentimiento adecuados
- Distribuir spam o comandos desde el dispositivo infectado para afectar a otros dispositivos o redes
- Estafar al usuario

Una aplicación, un objeto binario o una modificación al marco de trabajo pueden ser Potencialmente Dañinos y, por lo tanto, generar un comportamiento malicioso, aunque no estén diseñados para causar daño. Esto sucede porque es posible que las aplicaciones, los objetos binarios o las modificaciones del marco de trabajo funcionen de manera diferente según

diversas variables. Por lo tanto, lo que es perjudicial para un dispositivo Android podría no plantear ningún riesgo para otro dispositivo Android. Por ejemplo, un dispositivo que ejecuta la última versión de Android no se ve afectado por aplicaciones dañinas que usan API obsoletas para provocar un comportamiento malicioso, pero sí podría estar en riesgo un dispositivo que ejecuta una versión de Android mucho más antigua. Las aplicaciones, los objetos binarios y las modificaciones del marco de trabajo se marcan como software malicioso o APD si claramente plantean un riesgo para todos los dispositivos y usuarios de Android.

Las categorías de software malicioso que se incluyen a continuación reflejan nuestra firme convicción de que los usuarios deben comprender cómo se aprovechan sus dispositivos y promover un ecosistema seguro que permita una sólida innovación y una experiencia confiable del usuario.

Visita [Google Play Protect](#) para obtener más información.

Puerta trasera

Se trata de código que permite que se ejecuten operaciones no deseadas, potencialmente dañinas y controladas de forma remota en un dispositivo.

Estas operaciones incluyen un comportamiento que colocaría a la aplicación, el objeto binario o la modificación del marco de trabajo dentro de una de las otras categorías de software malicioso en caso de que se ejecuten automáticamente. En general, la puerta trasera es una descripción de cómo puede ocurrir una operación potencialmente dañina en un dispositivo y, por lo tanto, no está totalmente alineada con categorías como fraude en la facturación o software espía comercial. Como resultado, en determinadas circunstancias, Google Play Protect trata a un subconjunto de puertas traseras como una vulnerabilidad.

Fraude en la facturación

Se trata de código que procesa un cobro al usuario de manera intencionalmente engañosa.

El fraude en la facturación de telefonía celular se divide en fraude por SMS, fraude mediante llamadas y fraude en tarifa.

Fraude por SMS

Se trata de código que les cobra a los usuarios por el envío de SMS premium sin su consentimiento o que intenta disimular las actividades de SMS ocultando acuerdos de divulgación o mensajes SMS del operador de telefonía móvil que le notifican al usuario sobre los cargos o confirman las suscripciones.

Parte de este código, si bien técnicamente divulga el comportamiento de envío de SMS, incorpora comportamiento adicional que da lugar al fraude por SMS. Algunos ejemplos incluyen ocultarle al usuario partes de un acuerdo de divulgación, dificultar su lectura y suprimir de

forma condicional mensajes SMS del operador de telefonía móvil en los que se le informa al usuario sobre los cargos o se confirma una suscripción.

Fraude mediante llamadas

Se trata de código que genera cobros a los usuarios mediante llamadas a números premium sin su consentimiento.

Fraude en tarifa

Se trata de código que engaña al usuario para que se suscriba a contenido o lo compre a través de la factura de telefonía móvil.

El fraude en tarifa incluye cualquier tipo de facturación, excepto las llamadas y los SMS premium. Algunos ejemplos de esto incluyen facturación directa del proveedor, punto de acceso inalámbrico (WAP) y transferencia de tiempo de comunicación de telefonía móvil. El fraude de WAP es el tipo de fraude en tarifa más predominante. Puede incluir engaño a los usuarios para que hagan clic en un botón de una versión de WebView transparente que se carga de manera silenciosa. Cuando se realiza la acción, se inicia una suscripción recurrente y suele piratearse el correo electrónico o SMS de confirmación para impedir que los usuarios noten la transacción financiera.

Software espía comercial

Se trata de código que transmite información personal del dispositivo sin el aviso o consentimiento adecuados, y no muestra una notificación persistente de que esto está ocurriendo.

Las aplicaciones de software espía comercial transmiten datos a un tercero que no es el proveedor de la APD. Los padres pueden usar formas legítimas de estas aplicaciones para seguir a sus hijos. Sin embargo, estas aplicaciones no se pueden usar para rastrear a una persona (un cónyuge, por ejemplo) sin su conocimiento ni permiso si no se muestra una notificación persistente mientras se transmiten los datos.

Denegación del servicio (DoS)

Se trata de código que, sin el conocimiento del usuario, ejecuta un ataque de denegación del servicio (DoS) o es parte de un ataque de DoS contra otros sistemas y recursos.

Por ejemplo, esto puede ocurrir cuando se envía una gran cantidad de solicitudes HTTP para producir una carga excesiva en servidores remotos.

Aplicaciones de descarga hostil

Se trata de código que no es potencialmente dañino en sí, pero que descarga otras APD.

El código puede ser de descarga hostil de contenido si ocurre lo siguiente:

Hay motivos para creer que se creó con el fin de extender APD y descargó APD o contiene código que podría descargar e instalar aplicaciones.
Al menos el 5% de las aplicaciones descargadas por este son APD con un umbral mínimo de 500 descargas de aplicaciones observadas (25 descargas de APD observadas).

No se considera que los navegadores ni las aplicaciones de archivos compartidos más significativos sean de descarga hostil siempre que ocurra lo siguiente:

No activan descargas sin la interacción del usuario.
Todas las descargas de APD se inician si el usuario da su consentimiento.

Amenaza no relacionada con Android

Se trata de código que contiene amenazas no relacionadas con Android.

Estas aplicaciones no pueden causar daño a los dispositivos ni usuarios de Android, pero contienen componentes potencialmente dañinos para otras plataformas.

Suplantación de identidad (phishing)

Se trata de código que pretende provenir de una fuente confiable, solicita las credenciales de autenticación o los datos de facturación de un usuario y envía la información a un tercero. Esta categoría también se aplica al código que intercepta la transmisión de las credenciales de usuario en tránsito.

La suplantación de identidad (phishing) suele estar orientada a credenciales bancarias, números de tarjetas de crédito y credenciales de cuentas en línea para redes sociales y juegos.

Abuso de privilegios altos

Se trata de código que compromete la integridad del sistema ya que rompe la zona de prueba de la aplicación, obtiene privilegios altos o cambia o inhabilita el acceso a funciones básicas relacionadas con la seguridad.

Los siguientes son algunos ejemplos:

Aplicaciones que no cumplen con el modelo de permisos de Android o que roban credenciales (p. ej., tokens de OAuth) de otras aplicaciones
Aplicaciones que abusan de las funciones para evitar que las desinstalen o las detengan
Aplicaciones que inhabilitan SELinux

Las aplicaciones de elevación de privilegios que otorgan a los dispositivos derechos de administrador sin permiso del usuario se clasifican como aplicaciones con derechos de administrador.

Ransomware

Se trata de código que toma el control parcial o extensivo de un dispositivo o sus datos y exige que el usuario realice un pago o una acción para liberar el control.

Algún ransomware encripta los datos en el dispositivo y exige el pago para desencriptarlos, o bien aprovecha las funciones administrativas del dispositivo de modo que no pueda quitarlo un usuario común. Los siguientes son algunos ejemplos:

- Bloquear a un usuario para que no pueda acceder al dispositivo y exigirle dinero para restablecer su control

- Encriptar datos en el dispositivo y exigir un pago, ostensiblemente, para desencriptarlos

- Implementar las funciones del Administrador de políticas del dispositivo y bloquear la posibilidad de eliminación por parte del usuario

Se trata de código que se distribuye con el dispositivo y cuyo fin principal es que la administración del dispositivo subsidiado se pueda excluir de la categoría de ransomware siempre y cuando cumpla satisfactoriamente con los requisitos de administración y bloqueo seguros, y con los de consentimiento y divulgación adecuada para el usuario.

Modificación de dispositivos para obtener permisos de administrador

Se trata de código que modifica el dispositivo para tener permisos de administrador.

Hay una diferencia en el código de este tipo cuando es malicioso y no malicioso. Por ejemplo, las aplicaciones que modifican el dispositivo para tener permisos de administrador con fines no maliciosos le notifican al usuario por adelantado que harán esto y no ejecutan otras acciones potencialmente dañinas que se apliquen a otras categorías de APD.

Las aplicaciones que modifican el dispositivo para tener permisos de administrador con fines maliciosos no le notifican al usuario que harán esto, o sí le informan por adelantado sobre el proceso pero también ejecutan otras acciones que se aplican a otras categorías de APD.

Spam

Corresponde a código que envía mensajes no solicitados a los contactos del usuario o usa el dispositivo como retransmisor de spam por correo electrónico.

Software espía

Se trata de código que transmite datos personales fuera del dispositivo sin la notificación ni el consentimiento adecuados.

Por ejemplo, la transmisión de la siguiente información que no se divulga o se presenta de manera inesperada al usuario es suficiente para que se considere como software espía:

- Lista de contactos

- Fotos y otros archivos que se guardan en la tarjeta SD, o que no pertenecen a la aplicación

- Contenido del correo electrónico del usuario
- Registro de llamadas
- Registro de SMS
- Historial web o favoritos del navegador predeterminado
- Información de los directorios de /datos/ de otras aplicaciones.

Los comportamientos que se puedan considerar como una forma de espiar al usuario también se pueden marcar como software espía. Un ejemplo son las grabaciones de audio o de llamadas realizadas al teléfono, o el robo de datos de aplicaciones.

Troyano

Se trata de código que parece benigno, como un juego que afirma ser solo un juego, pero que realiza acciones no deseadas contra el usuario.

Esta clasificación se suele usar en combinación con otras categorías de APD. Un troyano contiene un componente inocuo y un componente dañino oculto. Por ejemplo, un juego que envía SMS premium desde el dispositivo del usuario en segundo plano y sin que el usuario lo sepa.

Una nota sobre aplicaciones poco comunes

Las aplicaciones nuevas y exóticas se pueden clasificar como poco comunes si Google Play Protect no tiene suficiente información para considerarlas seguras. Esto no significa que la aplicación sea necesariamente dañina, pero tampoco se puede considerar segura sin un análisis más profundo.

Una nota sobre la categoría de puerta trasera

La clasificación por categorías de software malicioso de puerta trasera depende de cómo actúa el código. Para que cualquier código se clasifique como puerta trasera, debe permitir, como condición necesaria, un comportamiento que lo colocaría en una de las otras categorías de software malicioso si se ejecutara automáticamente. Por ejemplo, si una aplicación permite la carga de un código dinámico y este extrae mensajes de texto, se clasificará como software malicioso de puerta trasera.

No obstante, si una aplicación permite la ejecución de un código arbitrario y no existe ningún motivo para creer que la ejecución de este código se agregó para producir un comportamiento malicioso, entonces la aplicación se tratará como con una vulnerabilidad, no como software malicioso de puerta trasera, y se le solicitará al desarrollador que le coloque un parche.

No permitimos apps que contengan anuncios engañosos o invasivos. Los anuncios solo deben mostrarse dentro de la aplicación que los ofrece. Los anuncios que se muestran dentro de la app se consideran parte de ella y deben cumplir con todas nuestras políticas. Para consultar las políticas sobre anuncios de juegos de apuestas, haz clic [aquí](#).

Google Play admite varias estrategias de monetización en beneficio de los desarrolladores y usuarios, como la distribución paga, los productos integrados en la aplicación, las suscripciones y los modelos basados en anuncios. Para garantizar la mejor experiencia del usuario, le solicitamos que cumpla con estas políticas.

Pagos

Las aplicaciones que ofrecen compras directas desde ellas o en la tienda deben cumplir con los siguientes lineamientos:

Compras en la tienda: Los desarrolladores que cobren por las aplicaciones y las descargas de Google Play deben usar el sistema de pago de Google Play.

Compras directas desde la aplicación:

Los desarrolladores que ofrezcan productos dentro de un juego descargado de Google Play o que brinden acceso a contenido del juego deben usar la [Facturación integrada en Google Play](#) como forma de pago.

Los desarrolladores que ofrezcan productos dentro de otra categoría de aplicación descargada de Google Play deben usar la [Facturación integrada en Google Play](#) como forma de pago, excepto en los siguientes casos:

El pago es únicamente para productos físicos.

El pago corresponde a contenido digital que se puede usar fuera de la aplicación (por ejemplo, las canciones que se pueden escuchar en otros reproductores de música).

Las monedas virtuales integradas solo pueden usarse dentro del título (juego o aplicación) para el que se compraron.

Los desarrolladores no deben engañar a los usuarios sobre las aplicaciones ni sobre la funcionalidad, el contenido, los bienes o los servicios integrados en la aplicación que vendan. Si la descripción de tu producto en Google Play hace referencia a funciones integradas en la aplicación a las que se aplica un cargo específico o adicional, entonces debes notificar claramente a los usuarios que se requiere un pago para acceder a esas funciones.

Las aplicaciones que ofrecen mecanismos para recibir elementos virtuales aleatorizados a partir de una compra (p. ej., "cajas de botín") deben divulgar dichos elementos de forma clara antes de que se complete la compra.

Suscripciones

Como desarrollador, usted no debe engañar a los usuarios acerca de los servicios de suscripción o el contenido que ofrece en su aplicación. Es de vital importancia que se

comunique de forma clara en todas las promociones integradas en las aplicaciones, así como en las pantallas de presentación.

En su aplicación: Debe ser transparente con respecto a la oferta, lo cual incluye ser explícito en lo que respecta a las condiciones de la oferta, como el costo de la suscripción, la frecuencia del ciclo de facturación y si es necesario suscribirse para usar la app. Los usuarios no deberían tener que realizar ninguna acción adicional para revisar esta información.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

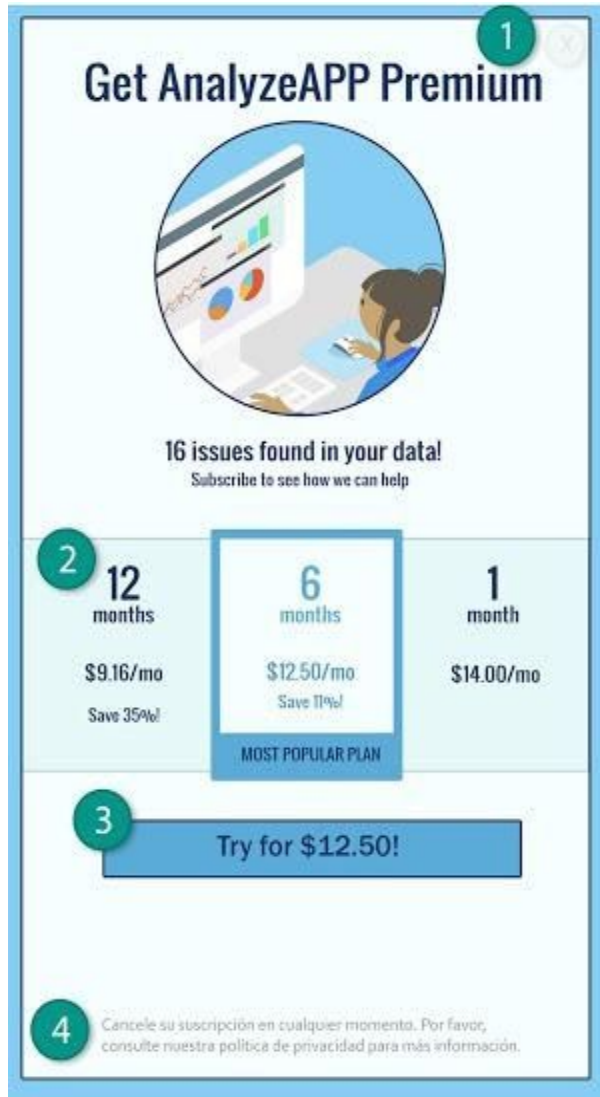
- Suscripciones mensuales que no informan a los usuarios que se les renovará el plan de forma automática y se les cobrará cada mes

- Suscripciones anuales que muestran sus precios de forma más prominente en términos del costo mensual

- Precios y condiciones de las suscripciones que no están totalmente localizados

- Promociones integradas en la aplicación que no demuestran con claridad que el usuario puede acceder al contenido sin una suscripción (cuando esté disponible)

- Nombres de SKU que no representan con precisión la naturaleza de la suscripción, como la etiqueta "Prueba gratuita" en una suscripción que tiene un cargo automático recurrente



- ① El botón para descartar no está claramente visible, por lo que es posible que los usuarios no comprendan que pueden acceder a la función sin aceptar la oferta de suscripción.
- ② La oferta solo muestra los precios en términos del costo mensual, por lo que es posible que los usuarios no comprendan que se les cobrarán seis meses en el momento de la suscripción.
- ③ La oferta solo muestra el precio de lanzamiento, por lo que es posible que los usuarios no comprendan cuánto se les cobrará automáticamente cuando finalice el período de lanzamiento.
- ④ La oferta se debe localizar al mismo idioma que los Términos y Condiciones, de manera que los usuarios puedan comprender la información completa.

Pruebas gratuitas y ofertas de lanzamiento

Antes de que se inscriba un usuario en su suscripción: Debe describir de manera clara y precisa los términos de su oferta, incluidos el precio, la duración y la descripción de los servicios o el

contenido a los que se dará acceso. Asegúrese de permitir que los usuarios tengan conocimiento de cuándo y cómo se convertirá una prueba gratuita en una suscripción pagada, cuánto costará la suscripción pagada y que pueden cancelarla si no quieren convertirse en suscriptores que pagan.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Ofertas que no explican de manera clara la duración de la prueba gratuita o del precio de lanzamiento

Ofertas que no explican de manera clara que se inscribirá de forma automática al usuario en una suscripción paga al final del período de oferta

Ofertas que no demuestran de forma clara que los usuarios pueden acceder al contenido sin una prueba (cuando está disponible esa opción)

Precios y condiciones de ofertas que no están completamente localizados

The image is a screenshot of a mobile app interface for 'AnalyzeAPP Premium'. It features a circular illustration of a person at a computer with data charts. Below the illustration, it says '16 issues found in your data! Subscribe to see how we can help'. A large blue button with a star icon says 'Try for free now!'. Below the button, there are four numbered callouts in green circles:

- 1 (top right corner)
- 2 (left of the button)
- 3 (left of the text: 'During your free trial, experience all of the great features our app can offer!')
- 4 (left of the text: 'Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.'

- ① El botón para descartar no está claramente visible, por lo que es posible que los usuarios no comprendan que pueden acceder a esta función sin registrarse para la prueba gratuita.
- ② La oferta hace hincapié en la prueba gratuita, por lo que es posible que los usuarios no comprendan que se les cobrará automáticamente un cargo al finalizar esa prueba.
- ③ La oferta no indica un período de prueba, por lo que es posible que los usuarios no comprendan cuánto tiempo durará el acceso gratuito a la suscripción.
- ④ La oferta se debe localizar al mismo idioma que los Términos y Condiciones, de manera que los usuarios puedan comprender la información completa.

Cancelación y administración de suscripciones

Como desarrollador, usted debe asegurarse de que su aplicación divulgue de forma clara cómo los usuarios pueden administrar o cancelar sus suscripciones.

Si un usuario cancela una suscripción adquirida en una aplicación que descargó de Google Play, la política establece que no recibirá un reembolso por el período de facturación vigente, pero seguirá recibiendo el contenido de la suscripción durante el resto del período de facturación actual, sin importar la fecha de cancelación. La cancelación entra en vigencia cuando finaliza el período de facturación actual.

Como proveedor de contenido o acceso, debe implementar una política de reembolso más flexible directamente con los usuarios. Es su responsabilidad notificarlos acerca de los cambios en las políticas de reembolso, cancelación y suscripción, y garantizar que estas cumplan con la ley aplicable.

No permitimos apps que contengan anuncios engañosos o invasivos. Los anuncios solo deben mostrarse dentro de la aplicación que los ofrece. Los anuncios que se muestran dentro de la app se consideran parte de ella y deben cumplir con todas nuestras políticas. Para consultar las políticas sobre anuncios de juegos de apuestas, haz clic [aquí](#).

No permitimos aplicaciones que contengan anuncios engañosos o invasivos. Los anuncios solo deben mostrarse dentro de la aplicación que los ofrece. Los anuncios que se muestran dentro de la app se consideran parte de ella y deben cumplir con todas nuestras políticas. Para consultar las políticas sobre anuncios de juegos de apuestas, haz clic [aquí](#).

Uso de Datos de Ubicación para los Anuncios

Las aplicaciones que aumentan el uso de datos de ubicación del dispositivo basados en permisos para publicar anuncios están sujetas a la política de [Información Personal y Sensible](#) y también deben cumplir con los siguientes requisitos:

El uso o la recopilación con fines publicitarios de los datos de ubicación del dispositivo basados en permisos deben estar claros para el usuario y documentados en la política de privacidad obligatoria de la aplicación, incluidos los vínculos a cualquier política de privacidad de redes publicitarias relevantes que aborde el uso de datos de ubicación.

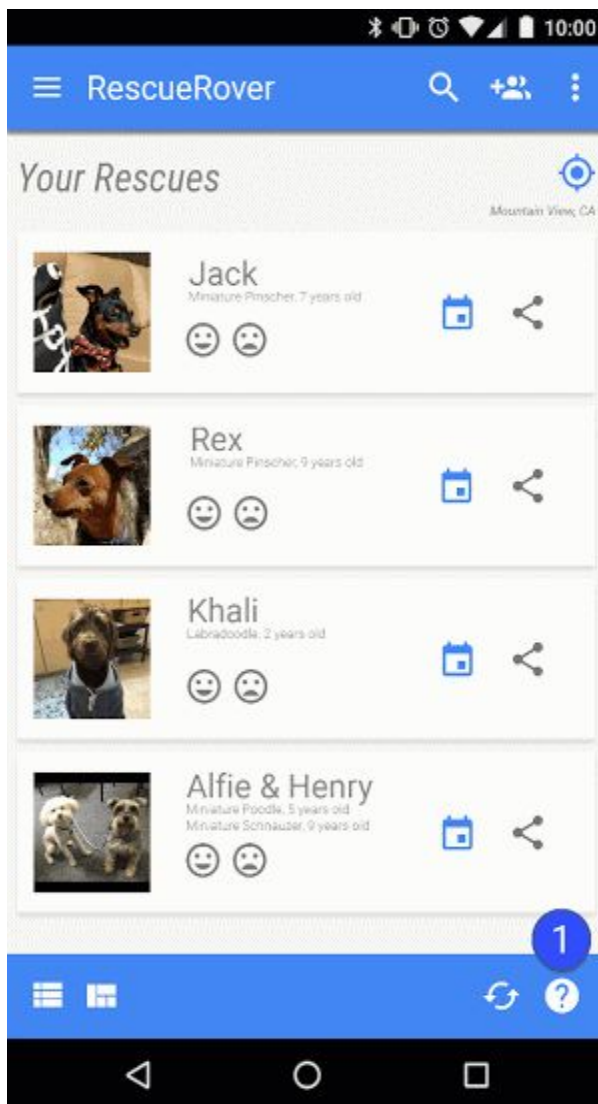
De acuerdo con los requisitos de [Permisos de Ubicación](#), solo pueden solicitarse permisos de ubicación para implementar servicios o funciones actuales dentro de la aplicación y no pueden solicitarse permisos de ubicación del dispositivo exclusivamente para el uso de anuncios.

Anuncios Engañosos

Los anuncios no deben imitar ni suplantar la interfaz de usuario de ninguna aplicación, así como tampoco las advertencias y notificaciones de un sistema operativo. El usuario debe saber a qué aplicación corresponde cada anuncio con claridad.

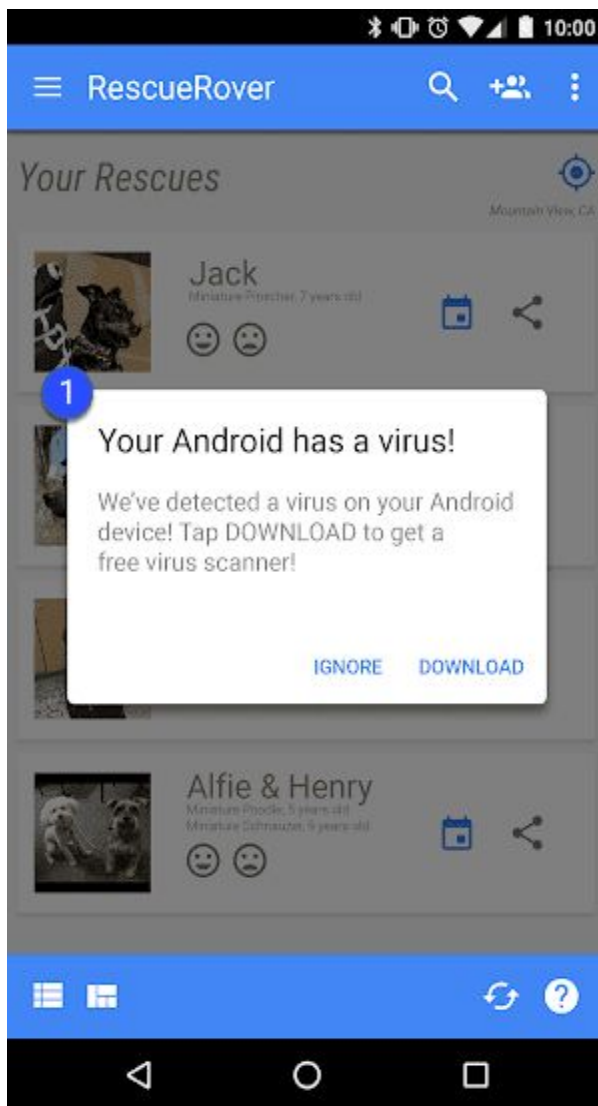
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

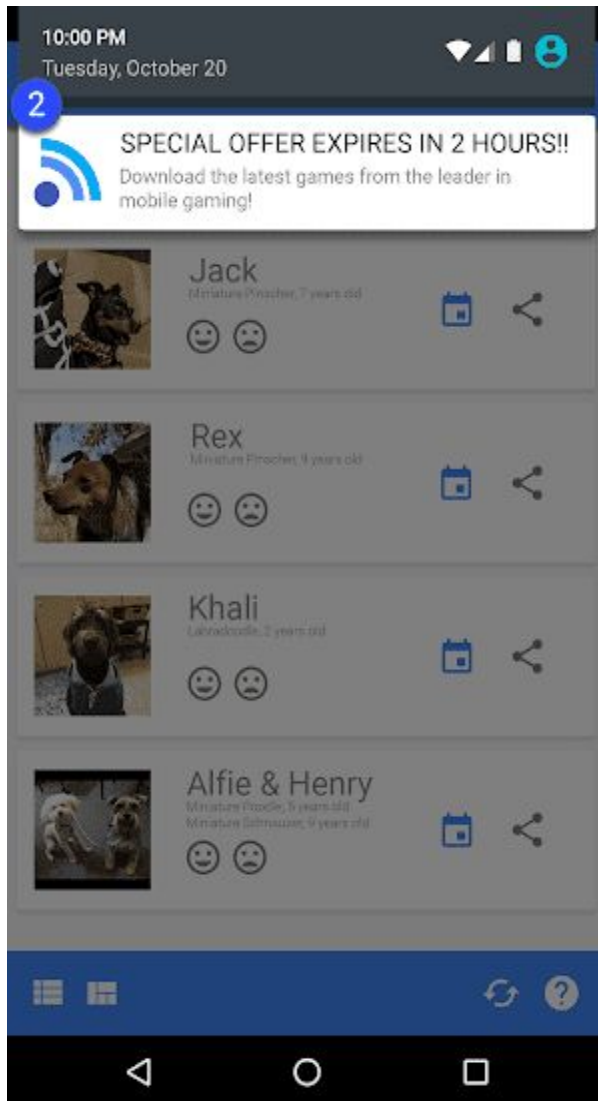
Anuncios que imitan la IU de una aplicación:



① El ícono de signo de interrogación en esta aplicación es un anuncio que lleva al usuario a una página de destino externa.

Anuncios que imitan una notificación del sistema:





① ② Los ejemplos anteriores muestran la forma en la que los anuncios imitan las notificaciones de varios sistemas.

Monetización de la Pantalla Bloqueada

A menos que el propósito exclusivo de la aplicación sea bloquear la pantalla, las aplicaciones no pueden incluir anuncios ni funciones que moneticen la pantalla bloqueada de un dispositivo.

Anuncios Invasivos

Los anuncios no deben mostrarse de manera tal que los usuarios hagan clic en ellos de forma involuntaria. Se prohíbe obligar a un usuario a hacer clic en un anuncio o enviar información personal con fines publicitarios antes de que puedan usar una aplicación de forma completa.

Los anuncios intersticiales solo pueden mostrarse dentro de la aplicación que los incluye. Si la aplicación muestra anuncios intersticiales o algún otro tipo de anuncios que interfieran con el uso normal, estos deben poder descartarse fácilmente sin sanciones.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Anuncios que ocupan toda la pantalla o interfieren con el uso normal y que no ofrecen una manera clara de descartar el anuncio:



① Este anuncio no tiene un botón para descartar.

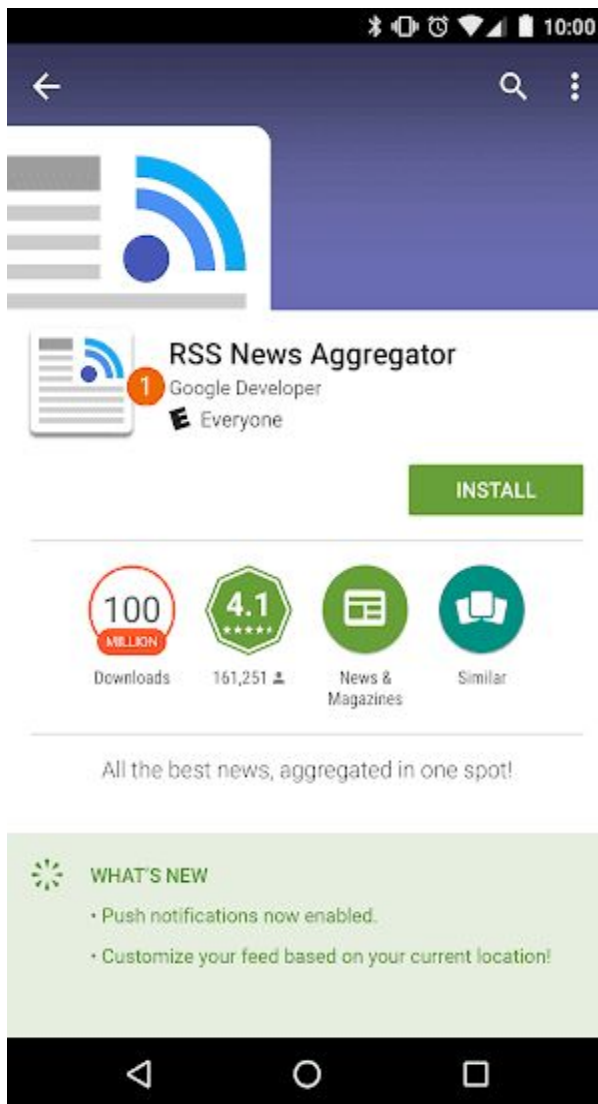
Interferencia con Aplicaciones, Anuncios de Terceros y la Funcionalidad del Dispositivo

Los anuncios asociados a la aplicación no deben interferir con otras aplicaciones, otros anuncios ni la operación del dispositivo, incluidos los botones y puertos del dispositivo o el sistema. Entre estos aspectos, se incluyen las superposiciones, las funciones complementarias

y los bloques de anuncios con widgets. Los anuncios solo deben mostrarse dentro de la aplicación que los ofrece.

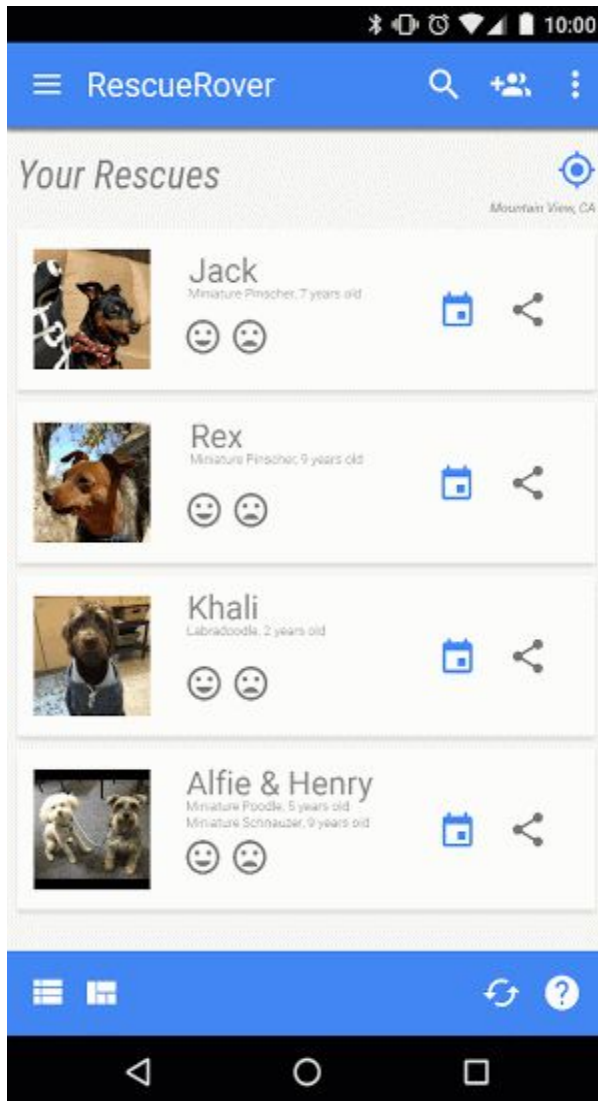
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Anuncios que se muestran fuera de la aplicación que los ofrece:



Descripción: El usuario navega a la pantalla principal desde esta aplicación, y un anuncio aparece en dicha pantalla de manera repentina.

Anuncios que se activan por medio del botón de la pantalla principal u otras funciones diseñadas específicamente para salir de la aplicación:

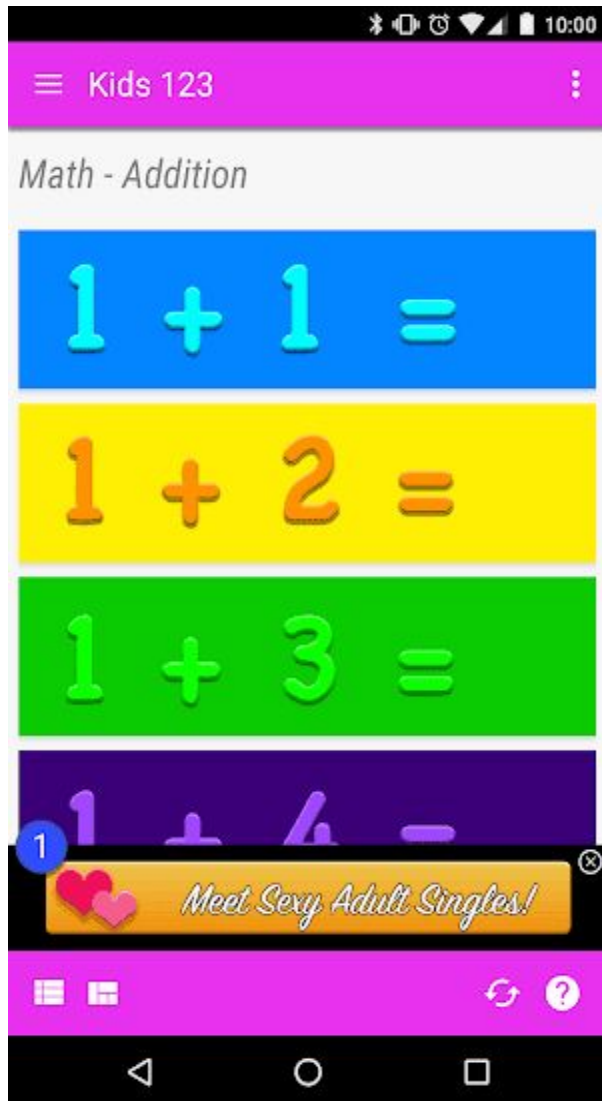


Descripción: El usuario intenta salir de la aplicación y navegar a la pantalla principal, pero un anuncio interrumpe el flujo esperado.

Anuncios Inapropiados

Los anuncios que muestre la aplicación deben ser adecuados para el público al que se orienta, incluso si el contenido cumple con nuestras políticas.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.



① El anuncio es inapropiado para el público al que está orientada esta aplicación.

Uso del ID de Publicidad de Android

La versión 4.0 de los Servicios de Google Play introdujo nuevas API y un ID para que lo usen los proveedores de publicidad y análisis. Las condiciones para el uso de este ID se encuentran a continuación.

Uso. El identificador de publicidad de Android solo debe usarse para la publicidad y el análisis del usuario. El estado de la configuración para inhabilitar la publicidad basada en intereses o cancelar la personalización de anuncios se debe verificar cada vez que se ingrese el ID.

Asociación con información de identificación personal u otros identificadores. El identificador de publicidad no debe conectarse a información de identificación personal ni asociarse con cualquier identificador de dispositivo persistente (por ejemplo, SSAID, dirección MAC, IMEI, etc.) sin el consentimiento explícito del usuario.

Respeto de las selecciones de los usuarios. Si se realiza el restablecimiento, un nuevo identificador de publicidad no debe estar conectado a uno anterior ni a datos derivados de un identificador de publicidad previo sin el consentimiento explícito del usuario. Además, debe respetar la configuración de la opción de "inhabilitar la publicidad basada en intereses" o "Cancelar personalización de anuncios" que haya seleccionado un usuario. Si un usuario habilitó esta configuración, no podrá usar el identificador de publicidad para crear perfiles de usuario con fines publicitarios ni para orientarse a los usuarios con anuncios personalizados. Las actividades permitidas incluyen la publicidad contextual, la limitación de frecuencia, el seguimiento de conversiones, la información y seguridad, y la detección de fraudes.

Transparencia para los usuarios. La recopilación y el uso del identificador de publicidad, y el compromiso con estas condiciones deben darse a conocer a los usuarios en un aviso de privacidad legalmente adecuado. Para obtener información sobre nuestros estándares de privacidad, revisa nuestra política de [Datos del Usuario](#).

Cumplimiento de las condiciones de uso. El identificador de publicidad solo puede utilizarse de acuerdo con estas condiciones. Lo mismo se espera de cualquier tercero con quien se comparta durante el transcurso del negocio. Todas las aplicaciones que se suban a Google Play o se publiquen en esa plataforma deben usar el ID de publicidad (cuando esté disponible en el dispositivo) en lugar de cualquier otro identificador de dispositivo para fines publicitarios.

Programa de anuncios para familias

Si publicas anuncios en la aplicación y esta se orienta únicamente a niños según se describe en la [Política de Familias](#), debes usar SDK de anuncios que cumplan con la autocertificación relacionada con las políticas de Google Play, incluso con los requisitos de certificación de SDK de anuncios que se incluyen a continuación. Si el público objetivo de tu aplicación incluye tanto niños como usuarios mayores, debes implementar medidas para filtrar por edad y asegurarte de que los anuncios que se muestren a los niños provengan exclusivamente de uno de los SDK de anuncios autocertificados. Las aplicaciones que participan en el programa Designed for Families solo pueden usar SDK de anuncios autocertificados.

Solo se requiere el uso de SDK de anuncios certificados por Google Play si usas SDK para mostrar anuncios a niños. Si bien eres responsable de garantizar que el contenido del anuncio y las prácticas de recopilación de datos cumplan con la [Política de Datos del Usuario](#) y la [Política de Familias](#) de Play, se permite lo siguiente sin el requisito de autocertificación de SDK de anuncios ante Google Play:

- Publicidad interna en la que uses SDK para administrar la promoción cruzada de tus apps o productos y otros medios de tu propiedad

- Participación en ofertas directas con anunciantes y uso de SDK para la administración de inventario

Requisitos de certificación de SDK de anuncios

Define el significado de comportamientos y contenido de anuncio reprochables, y prohíbelos en las condiciones o políticas de los SDK de anuncios. Las definiciones no deben derivar en un incumplimiento de las Políticas del Programa para Desarrolladores de Google Play.

Crea un método para clasificar las creatividades de los anuncios en función de los grupos etarios adecuados; incluye, como mínimo, los grupos "Apto para todo público" y "Mayores de edad". La metodología de clasificación debe estar alineada con la metodología que proporciona Google a los SDK una vez que se complete el formulario de interés que se incluye a continuación.

Permita que los publicadores soliciten contenido dirigido a niños para la publicación de anuncios por solicitud o por aplicación. Dicho contenido debe cumplir con las leyes y normas aplicables, como la [Ley de Protección de la Privacidad Infantil en Internet \(COPPA\) de los EE.UU.](#) y el [Reglamento General de Protección de Datos \(GDPR\)](#) de la UE. Google Play también exige la inhabilitación de anuncios personalizados, publicidad basada en intereses y remarketing como parte del contenido dirigido a niños.

Asegúrate de que se usen ofertas en tiempo real para mostrar anuncios a los niños, que se hayan revisado las creatividades y que se propaguen los indicadores de privacidad a los ofertantes.

Proporciona suficiente información a Google para que pueda verificar que los SDK de anuncios cumplen con todos los requisitos para la certificación, y responde de forma oportuna a cualquier solicitud de información adicional.

Nota: Los SDK de anuncios deben admitir un proceso de publicación de anuncios que cumpla con todos los estatutos y normas relevantes relacionados con niños que podrían aplicarse a sus publicadores.

Requisitos de mediación para las plataformas de publicación cuando se publican anuncios dirigidos a niños:

Usa únicamente SDK de anuncios certificados por Google Play o implementa las protecciones necesarias para garantizar que todos los anuncios que se publiquen desde redes de mediación cumplan con estos requisitos.

Ofrece las señales necesarias para indicar la clasificación del contenido del anuncio y cualquier contenido dirigido a niños que corresponda.

Si eres desarrollador, puedes consultar esta [lista de SDK de anuncios autocertificados](#).

También puede compartir este [formulario de interés](#) con SDK de anuncios que deseen autocertificarse.

Ficha de Play Store y promociones

La promoción y la visibilidad de una aplicación afectan la calidad de Play Store de manera radical. Por este motivo, no incluya fichas de Play Store que generen spam, promociones de baja calidad o medios para aumentar la visibilidad de una aplicación en Google Play artificialmente.

Promoción de aplicaciones

No se permite la publicación de aplicaciones que, de forma directa o indirecta, participen en prácticas de promoción engañosas o perjudiciales para los usuarios o el ecosistema de desarrolladores, o que se beneficien de ellas. Esto incluye las aplicaciones que tengan los comportamientos que se detallan a continuación:

- El uso de anuncios engañosos en sitios web, aplicaciones y otras propiedades, lo que incluye las notificaciones que sean similares a las del sistema y alertas

- Las tácticas de promoción o de instalación que redirijan a los usuarios a Google Play o a descargar aplicaciones sin previo aviso sobre la acción

- La promoción no solicitada mediante servicios por SMS.

Es tu responsabilidad garantizar que todas las redes de publicidad o afiliados que estén asociados con la aplicación cumplan con estas políticas y no participen de ninguna práctica de promoción que esté prohibida.

Metadatos

No se permiten aplicaciones con metadatos engañosos, no descriptivos, irrelevantes, excesivos, inapropiados ni con formato inadecuado, entre los que se incluyen, sin limitarse a ello, la descripción de la aplicación, el nombre del desarrollador, el título, el ícono, las capturas de pantalla y las imágenes promocionales. Los desarrolladores deben proporcionar una descripción clara y bien escrita. En la descripción de la aplicación, tampoco se permiten testimonios de usuarios anónimos ni sin la atribución correspondiente.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.



- ① Testimonios de usuarios anónimos o sin la atribución correspondiente
- ② Comparación de datos de aplicaciones o marcas
- ③ Bloques de palabras y listas de palabras verticales/horizontales

Los siguientes son ejemplos de textos, imágenes o videos inapropiados que no deben incluirse en una ficha de Play Store:

Imágenes o videos con contenido de carácter sexual. No incluya imágenes con contenido provocativo, como pechos, nalgas, genitales o cualquier contenido anatómico vulgarizado, tanto real como ilustrado.

Lenguaje inapropiado para el público general. No incluya lenguaje ofensivo o vulgar en la ficha de la aplicación. Si se trata de un elemento fundamental, se debe censurar la presentación en la ficha de Play Store.

Violencia gráfica o representada de manera explícita en íconos de aplicaciones, videos o imágenes promocionales.

Representaciones del uso de drogas ilegales. Incluso el contenido de carácter educativo, documental, científico o artístico debe ser apto para todo público en la ficha de Play Store.

A continuación, se detallan algunas prácticas recomendadas:

Destaca lo mejor de la aplicación. Comparte hechos interesantes para que los usuarios entiendan qué tiene de especial.

Asegúrate de que el título y la descripción de la aplicación describan su funcionalidad de forma precisa.

Evita el uso de palabras clave o referencias que sean repetitivas o que no estén relacionadas con la aplicación.

Use una descripción breve y directa. Por lo general, las descripciones cortas ofrecen una mejor experiencia del usuario, especialmente en los dispositivos con pantallas pequeñas. El uso de repeticiones, formato inadecuado y longitud o detalles excesivos puede resultar en el incumplimiento de esta política.

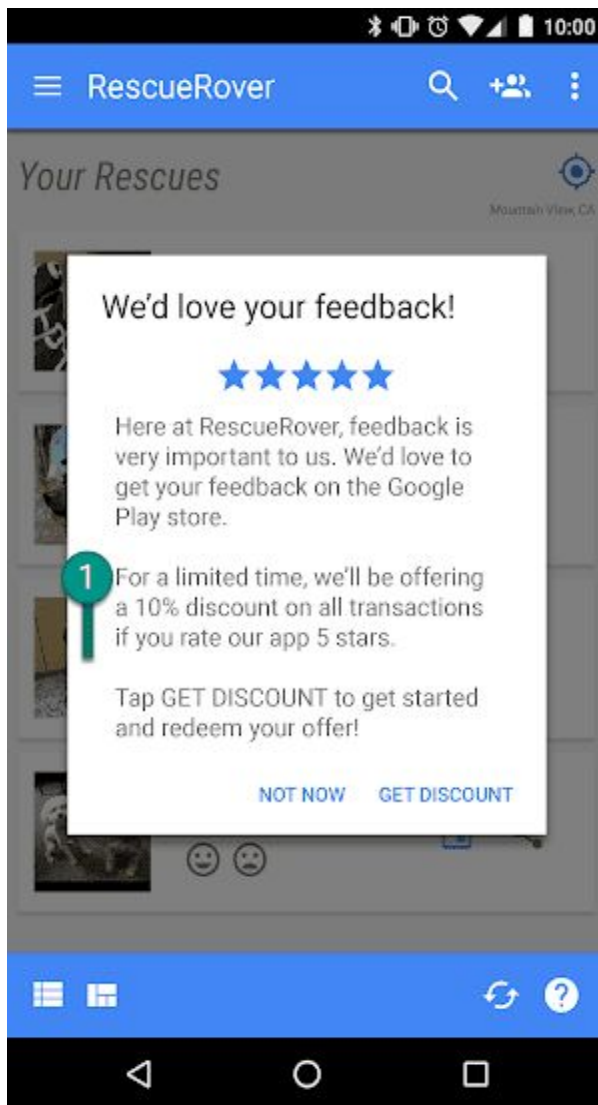
Recuerda que la ficha debe ser apta para todo público. Evita el uso de texto, imágenes o videos inapropiados en la ficha, y cumple con los lineamientos mencionados.

Calificaciones, instalaciones y opiniones de usuarios

Los desarrolladores no deben manipular la posición de las aplicaciones en Google Play. Entre otros aspectos, esto incluye el aumento de la cantidad de opiniones, instalaciones o calificaciones de productos a través de medios ilegítimos, como instalaciones, calificaciones y opiniones fraudulentas o que se hayan incentivado.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

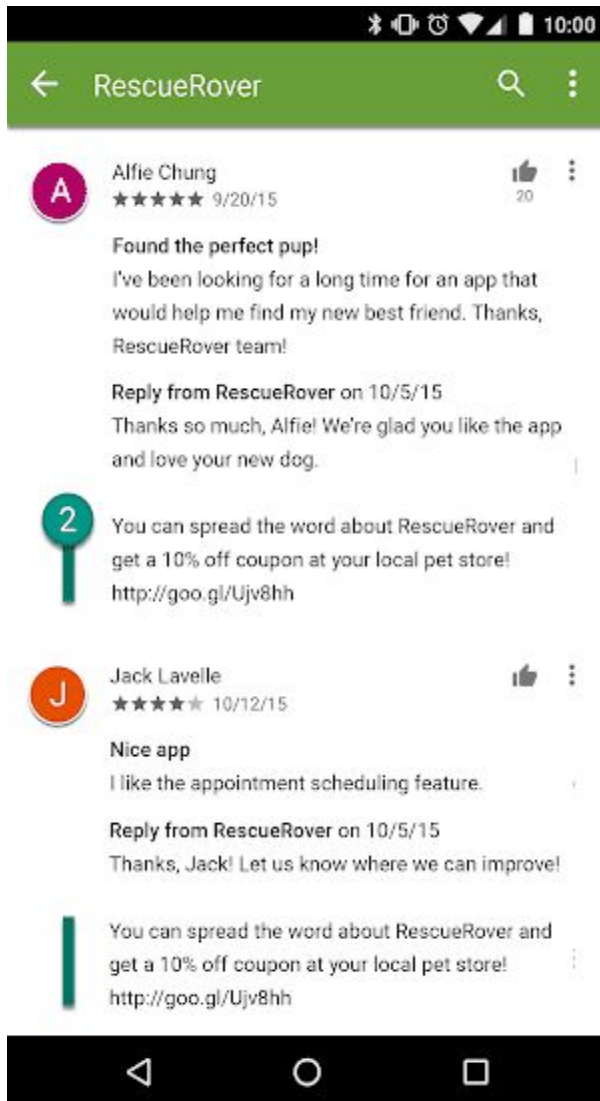
Solicitarles a los usuarios que califiquen una aplicación a cambio de un incentivo:



① Esta notificación ofrece a los usuarios un descuento a cambio de una calificación alta.

Enviar calificaciones de forma reiterada para influir en la posición de la aplicación en Google Play

Enviar o motivar a los usuarios a que envíen opiniones que incluyan contenido inapropiado, como afiliados, cupones, códigos de juegos, direcciones de correo electrónico o vínculos a otras aplicaciones o sitios web



② Esta opinión motiva a los usuarios a promocionar la aplicación de RescueRover a cambio de una oferta de cupón.

Las calificaciones y opiniones representan la calidad de una aplicación. Los usuarios deben considerarlas auténticas y relevantes. A continuación, se detallan algunas de las prácticas recomendadas a la hora de responder la opinión de un usuario:

Asegúrese de que la respuesta se centre en el problema que se indica en los comentarios del usuario y no solicite una calificación superior.
Se deben incluir referencias a recursos útiles, como una dirección de asistencia o una página de preguntas frecuentes.

Clasificaciones del contenido

Nuestro sistema de clasificación del contenido incluye clasificaciones oficiales de la [Coalición Internacional de Clasificación por Edad \(IARC\)](#) y está diseñado para ayudar a los

desarrolladores a comunicar las clasificaciones del contenido a los usuarios en función de la relevancia a nivel local.

Cómo se usan las clasificaciones del contenido

Las clasificaciones del contenido se usan para informar a los consumidores, especialmente a los padres, sobre el contenido potencialmente cuestionable que existe en una aplicación. También ayudan a filtrar o bloquear el contenido en ciertos territorios o a usuarios específicos cuando lo exige la ley; además, determinan la elegibilidad de una aplicación para participar en programas especiales para desarrolladores.

Cómo se determina la clasificación del contenido

Para recibir una clasificación del contenido, primero debe completar un [cuestionario de clasificación en Play Console](#) acerca de las características del contenido que incluyen sus aplicaciones. En función de las respuestas al cuestionario, se le asignará a la aplicación una clasificación del contenido de varias autoridades de clasificación. Debe proporcionar respuestas precisas en el cuestionario de clasificación del contenido. Las respuestas falsas sobre el contenido de la aplicación pueden resultar en su eliminación o suspensión.

Para evitar que la aplicación aparezca como "Sin clasificación", se debe completar el cuestionario de clasificación del contenido para cada aplicación nueva que se envíe a Play Console y para todas las aplicaciones existentes activas en Google Play. Se quitarán de Play Store las aplicaciones que no tengan una clasificación del contenido.

Si realiza cambios en el contenido o las funciones de la aplicación que afecten las respuestas del cuestionario de clasificación, debe completar un nuevo cuestionario en Play Console.

Visite el [Centro de ayuda](#) para obtener más información sobre las diferentes [autoridades de clasificación](#) y cómo completar el cuestionario de clasificación del contenido.

Apelación de clasificación

Si no estás de acuerdo con la clasificación asignada a la aplicación, puedes apelar directamente a la autoridad de clasificación de la IARC. Para hacerlo, usa el vínculo que aparece en el correo electrónico del certificado.

Spam y funcionalidad mínima

Como mínimo, las apps deben brindarles a los usuarios un nivel básico de funcionalidad y una experiencia del usuario adecuada. Las aplicaciones que fallan, que muestran un comportamiento inconsistente con la experiencia del usuario funcional o que solo publican spam para los usuarios o Google Play no contribuyen con la ampliación del catálogo de manera significativa.

Spam

No se permiten aplicaciones que envíen spam a los usuarios o a Google Play, como las que envían mensajes no solicitados o aplicaciones repetitivas y de baja calidad.

Spam a través de mensajes

No se permiten aplicaciones que envíen SMS, correos electrónicos ni ningún otro tipo de mensajes en nombre del usuario sin darle la posibilidad de confirmar el contenido y los destinatarios.

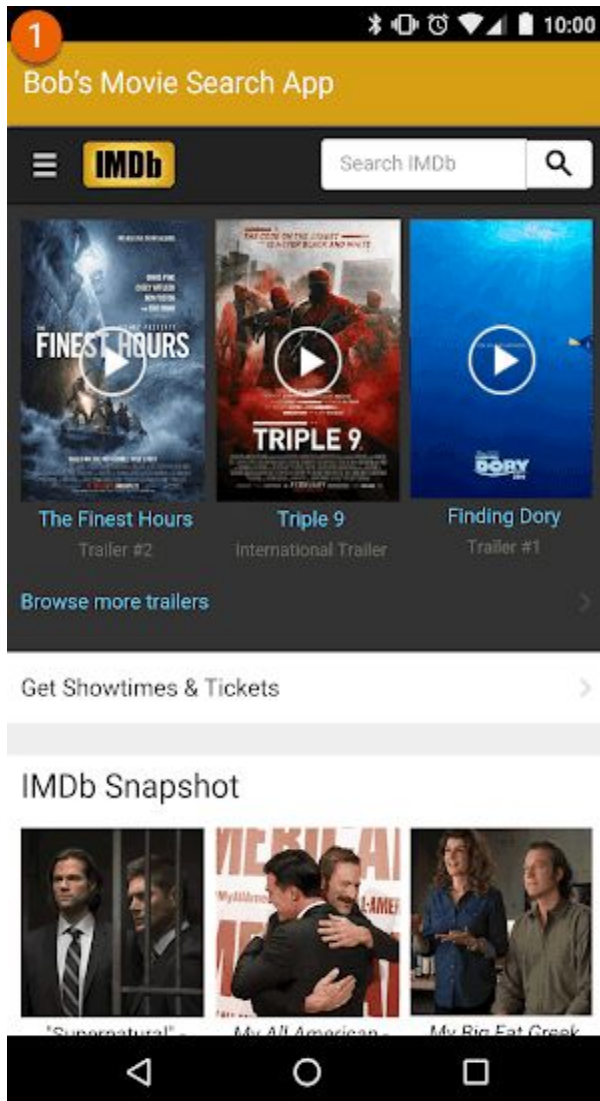
Spam de afiliados y de vistas web

No se permiten aplicaciones cuyo objetivo principal sea dirigir el tráfico afiliado a un sitio web o brindar una vista web de un sitio sin permiso del propietario o administrador del sitio web.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Una aplicación cuyo objetivo sea dirigir tráfico de referencia a un sitio web para recibir beneficios por los registros o compras del usuario en ese sitio

Aplicaciones cuyo objetivo principal sea proporcionar una vista web de un sitio sin permiso:



① Esta aplicación se llama “Aplicación de búsqueda de películas de Bob” y solo proporciona una vista web de IMDb.

Contenido repetitivo

No se permiten aplicaciones que solo brinden la misma experiencia que otras ya existentes en Google Play. Las aplicaciones deben proporcionar valor a los usuarios mediante la creación de contenido o servicios únicos.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Copiar elementos de otras aplicaciones sin agregar contenido o valor original

Crear varias aplicaciones con un contenido y una experiencia del usuario muy similares (si estas aplicaciones tienen poco volumen de contenido, los desarrolladores deben considerar la creación de una sola aplicación que incluya todo el contenido)

No se permiten aplicaciones creadas con una herramienta automatizada o un servicio de asistente, o que se basen en plantillas y que el operador de ese servicio las envíe a Google Play en nombre de terceros. Solo se admite ese tipo de aplicaciones si se publican por medio de una cuenta de desarrollador individual registrada que pertenezca al usuario de la herramienta automatizada y no al operador del servicio.

Creadas para la publicación de anuncios

No se permiten las aplicaciones cuyo objetivo principal sea publicar anuncios.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Aplicaciones en las que se publican anuncios intersticiales luego de cada acción del usuario, incluidas, entre otras, las acciones para hacer clic, deslizar el dedo, etcétera.

Funcionalidad mínima

Asegúrate de que la aplicación brinde una experiencia del usuario estable, atractiva y responsiva.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Aplicaciones que no tienen ninguna función o que están diseñadas para no realizar ninguna acción

Funcionalidad dañada

No permitimos las aplicaciones que fallan, se cierran de manera forzada, se bloquean o funcionan de manera anormal.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Aplicaciones que no se instalan

Aplicaciones que se instalan, pero no se cargan

Aplicaciones que se cargan, pero no responden

Otros programas

Además de cumplir con las políticas de contenido que se establecen en este Centro de políticas, es posible que las aplicaciones que se diseñen para otras experiencias de Android y se distribuyan mediante Google Play estén sujetas a requisitos de políticas específicas del

programa. Por ello, asegúrese de revisar la lista que aparece a continuación para determinar si algunas de estas políticas son relevantes en su aplicación.

Apps instantáneas Android

Con las Apps instantáneas Android, queremos crear experiencias para el usuario fluidas y emocionantes que cumplan con los estándares más altos de privacidad y seguridad. Nuestras políticas están diseñadas para lograr ese objetivo.

Los desarrolladores que elijan distribuir Apps instantáneas Android a través de Google Play deberán cumplir con las siguientes políticas, además de todas las otras [Políticas del Programa para Desarrolladores de Google Play](#).

Identidad

En el caso de las apps instantáneas que incluyan la función de acceso, los desarrolladores deben integrar [Smart Lock para contraseñas](#).

Compatibilidad con vínculos

Es obligatorio que los desarrolladores de Apps instantáneas Android proporcionen correctamente los vínculos a otras aplicaciones. Si las apps instantáneas o instaladas del desarrollador contienen vínculos que pueden dirigir a una app instantánea, el desarrollador deberá enviar a los usuarios a esa app instantánea, en lugar de capturar los vínculos en una [WebView](#).

Especificaciones técnicas

Los desarrolladores deberán cumplir con las especificaciones técnicas y los requisitos de las Apps instantáneas Android que proporciona Google, que pueden modificar ocasionalmente, incluidos los que se indican en [nuestra documentación pública](#).

Ofrecimiento de instalación de aplicaciones

La app instantánea podrá ofrecerle al usuario la app instalable, pero este no deberá ser el objetivo principal. Cuando ofrezcan una instalación, los desarrolladores deberán hacer lo siguiente:

- Usar el [ícono "Obtener app" de material design](#) y la etiqueta "Instalar" para el botón de instalación.

- Tener más de 2 a 3 solicitudes de instalación implícita en la aplicación instantánea.

- Abstenerse de usar banners o cualquier otra técnica de tipo publicitario para presentar una solicitud de instalación a los usuarios.

Para obtener detalles adicionales sobre las apps instantáneas y los lineamientos de UX, consulte las [Prácticas recomendadas para la experiencia del usuario](#).

Cambios en el estado del dispositivo

Las apps instantáneas no deberán hacer cambios en el dispositivo de los usuarios que duren más que la sesión de la aplicación. Por ejemplo, no deberán cambiar el fondo de pantalla del dispositivo ni crear un widget en la pantalla principal.

Visibilidad de la aplicación

Los desarrolladores deberán asegurarse de que el usuario pueda ver las apps instantáneas de forma tal que esté al tanto en todo momento de que se están ejecutando en su dispositivo.

Identificadores de dispositivos

Se prohíbe el acceso de las apps instantáneas a identificadores del dispositivo que (1) persistan después de que la app instantánea haya dejado de ejecutarse y (2) el usuario no pueda restablecer. Entre otros ejemplos, se incluyen los siguientes:

- número de serie de la compilación
- direcciones MAC de cualquier chip de red
- códigos IMEI o IMSI

Las apps instantáneas podrán acceder al número de teléfono solo mediante el permiso de tiempo de ejecución. No se permite que los desarrolladores registren las huellas digitales del usuario mediante estos identificadores ni otros medios.

Tráfico de red

Se debe encriptar el tráfico de red desde la app instantánea con un protocolo TLS como HTTPS.

Familias

Google Play ofrece una plataforma valiosa a los desarrolladores para que muestren contenido acorde a las edades y de alta calidad para toda la familia. Antes de solicitar la inscripción de una aplicación en el programa Designed for Families o enviar una aplicación que se oriente a niños para su publicación en Google Play Store, usted es responsable de garantizar que esta sea adecuada para menores y que cumpla con todas las leyes relevantes.

[Obtenga más información sobre los procesos relacionados con el contenido para familias y consulte la lista de tareas interactiva en la Academia de apps.](#)

Cómo diseñar aplicaciones para niños y familias

A medida que aumenta el uso de la tecnología como herramienta para enriquecer las vidas de las familias, los padres buscan más contenido seguro y de alta calidad para compartir con sus hijos. Quizá sus aplicaciones estén diseñadas específicamente para niños o simplemente sean atractivas para ellos. Google Play quiere ayudarlo a garantizar que su aplicación sea segura para todos los usuarios, incluidas las familias.

La palabra "niños" puede tener distintos significados en diferentes regiones y contextos. Es importante que consulte a sus asesores legales a fin de determinar qué obligaciones o restricciones relacionadas con la edad pueden corresponder a su aplicación. Dado que usted conoce mejor que nadie cómo funciona, contamos con su ayuda a fin de garantizar que las aplicaciones de Google Play sean seguras para las familias.

Las aplicaciones que estén diseñadas específicamente para niños deben participar en el programa Designed for Families. Sin embargo, si los niños constituyen solo una parte de su público, participar en el programa Designed for Families sigue siendo una excelente manera de promover la aplicación para los usuarios adecuados. Incluso si decide no participar en el programa Designed for Families, debe cumplir con los requisitos de la Política de Familias de Google Play que se detallan a continuación, al igual que con todas las [Políticas del Programa para Desarrolladores de Google Play](#) y el [Acuerdo de Distribución para Desarrolladores](#).

Requisitos de Play Console

Público Objetivo y Contenido

En la sección [Público Objetivo y Contenido](#) de Google Play Console, debe indicar el público objetivo de su aplicación antes de publicarla. Para ello, seleccione uno de los grupos de edades disponibles. Independientemente de lo que seleccione en Google Play Console, si decide incluir en la aplicación terminología o imágenes dirigidas a niños, o que se puedan juzgar como tales, esto podría afectar la evaluación de Google Play sobre el público objetivo declarado. Google Play se reserva el derecho de revisar por su cuenta la información que usted brinde sobre la aplicación, a fin de determinar si el público objetivo declarado es el correcto.

Si selecciona un público objetivo que solo incluye adultos, pero Google determina que la selección es incorrecta porque la aplicación se orienta tanto a niños como a adultos, podrá aclararles a los usuarios que la aplicación no se orienta a niños si acepta incorporar una etiqueta de advertencia.

Solo debe seleccionar más de un grupo de edades como público objetivo de su aplicación si la diseñó para los usuarios que se incluyen en los grupos de edades seleccionados y se aseguró de que fuera apta para ellos. Por ejemplo, las aplicaciones diseñadas para bebés, niños pequeños y niños de edad preescolar solo deben tener seleccionado el grupo "Hasta 5 años" como público objetivo. Si la aplicación está diseñada para un nivel educativo específico, elija el grupo de edades que mejor represente ese nivel educativo. Solo debe seleccionar grupos de edades que incluyan niños y adultos si tiene la certeza de haber diseñado su aplicación para todas las edades.

Actualizaciones de la Sección "Público Objetivo y Contenido"

Podrá actualizar la información de su aplicación en la sección "Público Objetivo y Contenido" de Google Play Console en cualquier momento. Para que esta información se pueda ver reflejada en Google Play Store, primero se debe publicar una [actualización de la aplicación](#). Sin embargo, es posible que se revisen los cambios que realice en esta sección de Google Play Console a fin de garantizar que cumplan con las políticas, incluso antes de que se envíe la actualización de la aplicación.

Le recomendamos que les avise a los usuarios actuales si realiza algún cambio en el grupo de edades objetivo de su aplicación o si comienza a usar anuncios o compras directas desde ella, ya sea en la sección "Novedades" de la ficha de Play Store de la aplicación o mediante notificaciones dentro de ella.

Tergiversación en Play Console

La tergiversación de cualquier información relacionada con su aplicación en Play Console, incluida la sección "Público Objetivo y Contenido", puede causar que se elimine o suspenda la aplicación, por lo que es fundamental que proporcione información correcta.

Requisitos de la Política de Familias

Si los niños son parte del público objetivo de su aplicación, debe cumplir con los requisitos que se detallan a continuación. El incumplimiento de estos requisitos puede causar que se elimine o suspenda la aplicación.

1. Contenido de la aplicación: El contenido de la aplicación al que pueden acceder niños debe ser apto para ellos.
2. Respuestas en Google Play Console: Debe contestar de manera precisa en Google Play Console las preguntas relacionadas con su aplicación y actualizar las respuestas correspondientes para reflejar con exactitud cualquier cambio que realice en ella.
3. Anuncios: Si la aplicación muestra anuncios a niños o usuarios de edades desconocidas, deberá respetar los siguientes lineamientos:
 - usar únicamente [SDK de anuncios certificados por Google Play](#) para mostrar anuncios a esos usuarios
 - asegurarse de que los anuncios que se muestren a esos usuarios no incluyan publicidad basada en intereses ni remarketing
 - asegurarse de que los anuncios que se muestren a esos usuarios presenten contenido apropiado para niños
 - asegurarse de que los anuncios que se muestren a esos usuarios sigan los requisitos de formato del anuncio para Familias
 - garantizar el cumplimiento de todas las normativas legales aplicables y los estándares de la industria relacionados con la publicidad dirigida a niños
4. Recopilación de datos: Debe divulgar todo tipo de recopilación de [información personal y sensible](#) de los niños en su aplicación, incluidos los casos en que esta se recopile

mediante API o SDK que se invoquen o usen en la aplicación. La información sensible de los niños incluye, entre otros datos, información de autenticación, datos de los sensores del micrófono y la cámara, datos del dispositivo, ID de Android, ID de publicidad y datos de uso de los anuncios.

5. API y SDK: Debe asegurarse de que la aplicación implemente cualquier API y SDK de forma adecuada.

Las aplicaciones que se orienten únicamente a niños no deben contener API ni SDK cuyo uso no esté aprobado para servicios dirigidos a niños. Esto incluye el Acceso con Google (o cualquier otro Servicio de las API de Google que acceda a datos asociados con una Cuenta de Google), los Servicios de Juego de Google Play y cualquier otro Servicio de las API que use tecnología OAuth para la autenticación y autorización.

Las aplicaciones orientadas tanto a niños como a públicos mayores no deben implementar API ni SDK cuyo uso no esté aprobado para servicios dirigidos a niños, a menos que se usen detrás de una [pantalla neutral de comprobación de edad](#) o se implementen de una manera que no implique la recopilación de datos de niños (p. ej., ofrecer el Acceso con Google como una función opcional). Tenga en cuenta que todos los usuarios deben poder acceder a su aplicación, así como a una cantidad razonable de funciones.

6. Política de Privacidad: Debe proporcionar un vínculo a la política de privacidad de la aplicación en la página de la ficha de Play Store correspondiente. El vínculo se debe mantener activo mientras la aplicación esté disponible en Play Store y debe llevar a una política de privacidad que, entre otras cosas, describa correctamente cómo la aplicación recopila y usa los datos.

7. Restricciones especiales:

Si su aplicación usa realidad aumentada, debe incluir una advertencia de seguridad que aparezca tan pronto como se abra la sección de RA. La advertencia debe contener los siguientes elementos:

Un mensaje adecuado sobre la importancia de la supervisión parental

Un recordatorio sobre los riesgos físicos en el mundo real (p. ej., estar atento al entorno)

La aplicación no debe requerir el uso de un dispositivo no recomendado para niños (p. ej., Daydream, Oculus)

8. Cumplimiento Legal: Debe asegurarse de que la aplicación, incluidos todos los SDK o API que esta llame o use, cumpla con la [Ley de Protección de la Privacidad de Menores en Internet \(COPPA\) de los Estados Unidos](#), el [Reglamento General de Protección de Datos \(GDPR\) de la Unión Europea](#) y cualquier otra ley o norma aplicable.

Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

Aplicaciones que promueven juegos para niños en sus fichas de Play Store, pero cuyo contenido solo es apropiado para adultos

Aplicaciones que implementan API cuyas Condiciones del Servicio prohíben su uso en aplicaciones dirigidas a niños
Aplicaciones que idealizan el consumo de alcohol, tabaco o sustancias controladas
Aplicaciones que incluyen apuestas reales o simuladas
Aplicaciones que incluyen violencia, imágenes sangrientas o contenido ofensivo no apto para niños
Aplicaciones que proporcionan servicios de citas o que brindan consejos sexuales o asesoramiento matrimonial
Aplicaciones que muestran anuncios para mayores de edad a niños

Programa Designed for Families

Las aplicaciones que estén diseñadas específicamente para niños deben participar en el programa Designed for Families. Si su aplicación está diseñada para un público general, incluidos niños y familias, también puede solicitar participar en el programa.

Para que se acepte su aplicación en el programa, esta debe cumplir con todos los requisitos de la Política de Familias y los requisitos de elegibilidad de Designed for Families, además de los que se indican en las [Políticas del Programa para Desarrolladores de Google Play](#) y el [Acuerdo de Distribución para Desarrolladores](#).

Para obtener más información sobre el proceso que debe seguir para enviar su aplicación y solicitar su inclusión en el programa, haga clic [aquí](#).

Elegibilidad para el Programa

Todas las aplicaciones que participen en el programa Designed for Families deben incluir contenido de la aplicación y anuncios que sean relevantes y apropiados para niños y, además, satisfacer todos los requisitos que se detallan a continuación. Las aplicaciones que se acepten en el Programa Designed for Families deben mantenerse en pleno cumplimiento de todos los requisitos del programa. Google Play se reserva el derecho, a su entera discreción, de rechazar o quitar cualquier aplicación si determina que es inapropiada para el programa Designed for Families.

Requisitos de Designed for Families

1. Las aplicaciones deben estar clasificadas por la ESRB como "Aptas para todo público" o "Para mayores de diez años", o tener una clasificación equivalente.
2. Debe divulgar correctamente los elementos interactivos de la aplicación en el Cuestionario de Clasificación del Contenido de Google Play Console, incluidos los siguientes casos:
 - si los usuarios pueden interactuar o intercambiar información
 - si su aplicación comparte con terceros la información personal proporcionada por los usuarios
 - si la aplicación comparte la ubicación física del usuario con otros usuarios

3. si la aplicación usa la [API de Android Speech](#), se debe configurar el parámetro RecognizerIntent.EXTRA_CALLING_PACKAGE con su PackageName
4. Las aplicaciones solo deben usar [SDK de anuncios certificados por Google Play](#).
5. Las aplicaciones que estén diseñadas específicamente para niños no pueden solicitar permisos de ubicación.
6. Las aplicaciones deben usar el [Administrador de Dispositivo Complementario \(CDM\)](#) cuando soliciten Bluetooth, a menos que su aplicación se oriente únicamente a las versiones del sistema operativo (SO) del dispositivo no compatibles con CDM.
Aplicaciones que están clasificadas por la ESRB como "Aptas para todo público", pero contienen anuncios de juegos de apuestas
Aplicaciones para padres o cuidadores (p. ej, las dedicadas al seguimiento de la lactancia o guías sobre desarrollo)
Guías para padres o aplicaciones de administración de dispositivos diseñadas para que las usen únicamente padres o cuidadores

Categorías

Si se acepta la participación de su aplicación en el programa Designed for Families, puede elegir una segunda categoría específica para Familias que describa a su aplicación. A continuación, se indican las categorías disponibles para las aplicaciones que participan en el programa Designed for Families:

Acción y Aventura: Incluye aplicaciones y juegos de acción, desde juegos de carreras simples hasta aventuras de cuentos de hadas y otras aplicaciones y juegos diseñados para generar emoción.

Juegos de Mente: Incluye juegos de razonamiento, como rompecabezas, juegos de asociación, de preguntas y respuestas, y otros juegos de memoria, inteligencia o lógica.

Creatividad: Incluye aplicaciones y juegos que estimulan la creatividad, incluidas las aplicaciones de dibujo, pintura y codificación, así como otros juegos y aplicaciones en los que se puedan crear elementos.

Educación: Incluye aplicaciones y juegos diseñados con la colaboración de expertos del aprendizaje (p. ej., educadores, especialistas en aprendizaje, investigadores, etc.) para promover el aprendizaje académico, socioemocional, físico y creativo, así como el aprendizaje relacionado con conocimientos prácticos, el pensamiento crítico y la resolución de problemas.

Música y Video: Incluye aplicaciones y juegos con un componente de música o video, como las aplicaciones de simulación de instrumentos y aquellas que ofrecen contenido de audio de música o video.

Juegos Simbólicos: Incluye aplicaciones y juegos en los que el usuario puede simular que cumple una función, como cocinero, médico, príncipe o princesa, bombero, policía o un personaje ficticio.

Anuncios y monetización

Las políticas que se detallan a continuación se aplican a cualquier tipo de publicidad (tanto para sus aplicaciones como para las de terceros), oferta de compras directas desde la aplicación o cualquier otro tipo de contenido comercial (como colocaciones de productos pagadas) que se muestran a los usuarios de aplicaciones sujetas a los Requisitos de la Política de Familias y/o los Requisitos del Programa Designed for Families. Toda publicidad y oferta de compras directas desde la aplicación, así como el contenido comercial de estas aplicaciones, deben cumplir con las leyes y normas aplicables (incluidos los lineamientos autorreguladores o de la industria que sean relevantes).

Google Play se reserva el derecho de hacer cumplir la política a las aplicaciones que usen tácticas comerciales demasiado agresivas.

Requisitos del formato de los anuncios

Los anuncios y las ofertas de compras directas desde la aplicación no deberán incluir contenido engañoso ni estar diseñados de manera tal que los niños que usen la aplicación hagan clic en ellos de forma involuntaria. Están prohibidas las siguientes acciones:

- El uso de [paneles de anuncios](#)

- Anuncios que interfieran con el uso normal de la aplicación y que no se puedan cerrar después de cinco segundos

- Anuncios intersticiales y ofertas de compras directas desde la aplicación que se muestren inmediatamente después de que se abra la aplicación

- La colocación de varios anuncios en una misma página

- Anuncios y ofertas de compras directas desde la aplicación que no se distingan fácilmente del contenido de la aplicación

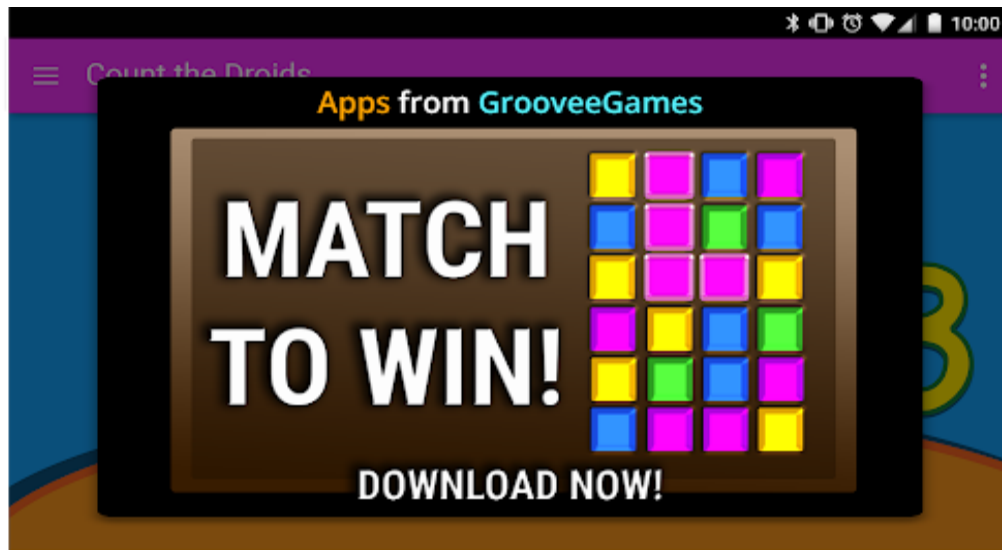
- Uso de tácticas ofensivas o emocionalmente manipuladoras para promover la visualización de anuncios o las compras directas desde la aplicación

- Falta de distinción entre el uso de monedas virtuales de juego y dinero real para hacer compras directas desde la aplicación

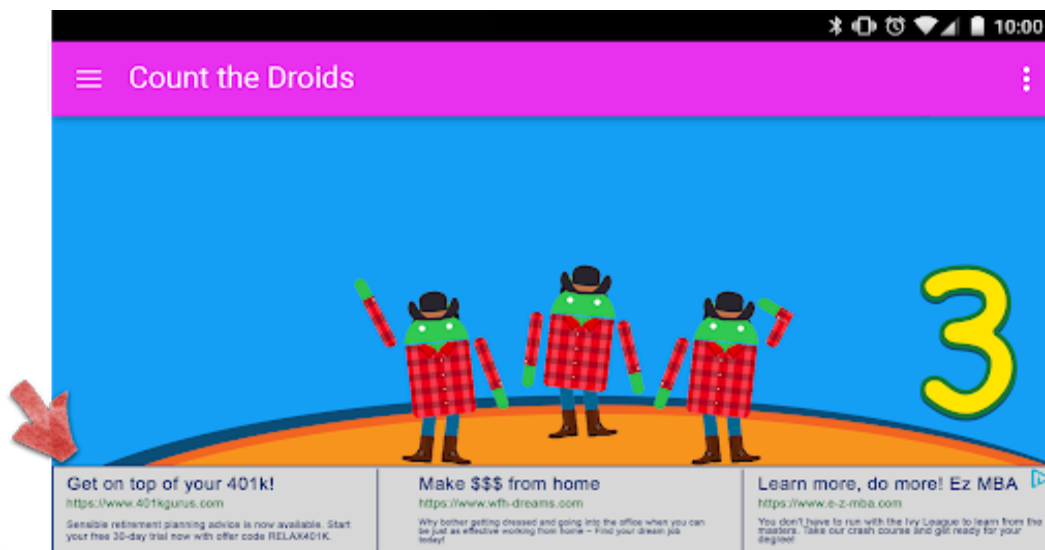
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Anuncios que se alejan del dedo del usuario cuando este trata de cerrarlos

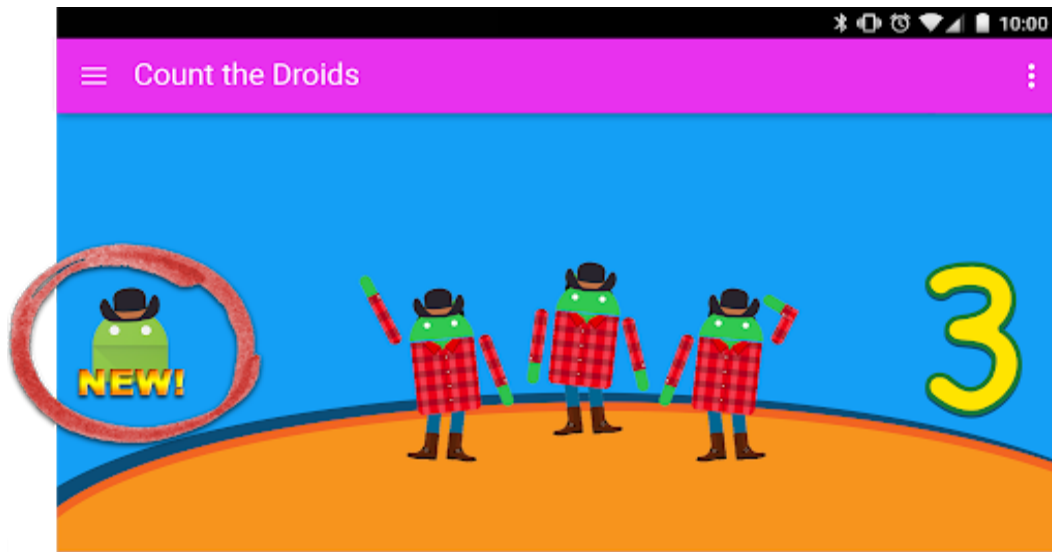
Anuncios que ocupan la mayor parte de la pantalla del dispositivo sin brindar al usuario una manera clara de descartarlo, como se muestra en el ejemplo a continuación:



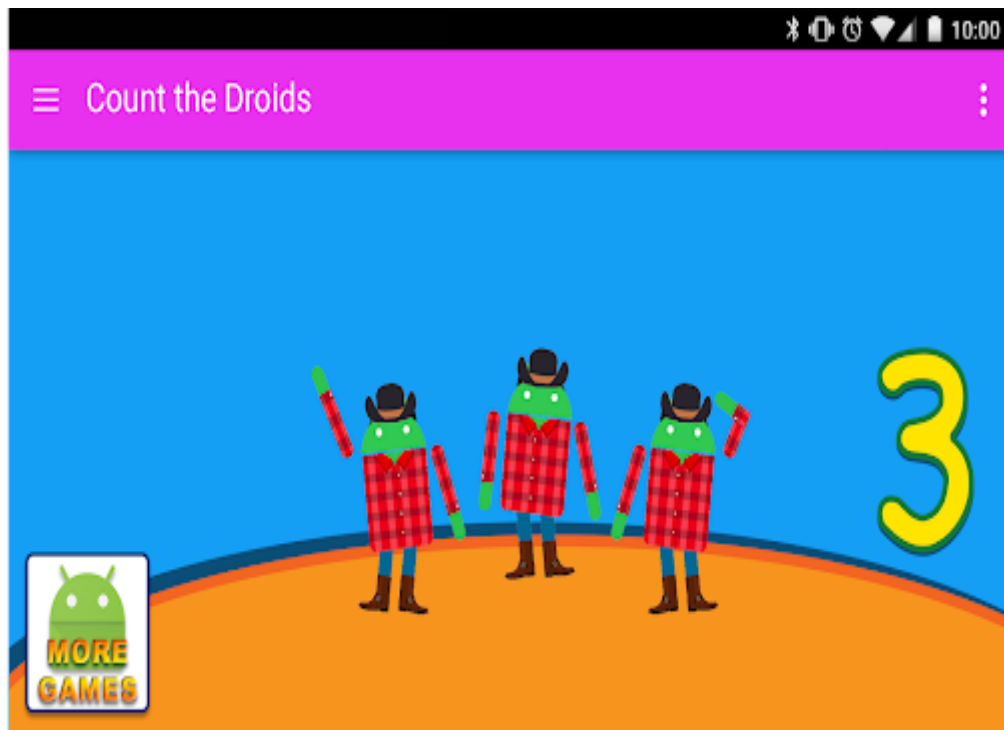
Anuncios de tipo banner que muestran varias ofertas, como en el ejemplo a continuación:



Anuncios que el usuario podría confundir con contenido de la aplicación, como se muestra en el ejemplo a continuación:



Botones o anuncios que promueven sus otras fichas de Google Play Store, pero que no se distinguen fácilmente del contenido de la aplicación, como se muestra en el ejemplo a continuación:



Los siguientes son ejemplos de contenido de anuncio inapropiado que no se debe mostrar a niños:

Contenido multimedia inapropiado: Incluye anuncios de programas de TV, películas, álbumes de música o cualquier otro medio de difusión que no sea apto para niños.

Videojuegos y software descargable inapropiados: Incluye anuncios de software y videojuegos electrónicos descargables que no sean aptos para niños.

Sustancias controladas o dañinas: Incluye anuncios sobre alcohol, tabaco, sustancias controladas o cualquier otra sustancia dañina.

Juegos de apuestas: Incluye anuncios que simulen juegos de apuestas, concursos o promociones de sorteos, aunque la participación sea gratuita.

Contenido adulto y sexualmente provocativo: Incluye anuncios con contenido sexual, provocativo o para mayores de edad.

Citas o relaciones: Incluye anuncios de sitios de citas o relaciones adultas.

Contenido violento: Incluye anuncios con contenido violento y explícito que no sea apto para niños.

SDK de anuncios

A la hora de publicar anuncios para niños, solo se pueden usar [SDK de anuncios certificados por Google Play](#). Las aplicaciones que participan en el programa Designed for Families solo pueden usar SDK de anuncios certificados por Google Play. Las aplicaciones que también se orienten a usuarios adultos podrán usar SDK de anuncios que no estén certificados, siempre y cuando haya una [pantalla neutral de comprobación de edad](#) en la aplicación y los SDK de anuncios que no estén certificados se usen únicamente para mostrar anuncios a usuarios verificados como adultos.

Consulta la página de la [política del Programa de Anuncios para Familias](#) a fin de obtener más detalles sobre estos requisitos y ver la lista actual de SDK de anuncios aprobados.

Si usas AdMob, consulta el [Centro de ayuda de AdMob](#) para obtener más detalles sobre sus productos.

Es tu responsabilidad garantizar que la aplicación satisfaga todos los requisitos relacionados con compras directas desde la aplicación, publicidad y contenido comercial. Comunícate con tus proveedores de SDK de anuncios para obtener más información acerca de sus políticas de contenido y prácticas publicitarias.

Compras directas desde la aplicación

Google Play volverá a autenticar a todos los usuarios antes de que se complete cualquier compra directa desde la aplicación en las aplicaciones que participen en el programa Designed for Families. El propósito de esta medida es ayudar a garantizar que quien apruebe las compras sea la parte que posee la responsabilidad financiera, no los niños.

Es mejor evitar el incumplimiento de una Política que tener que abordarlo. Sin embargo, en caso de incumplimiento, nos comprometemos a garantizar que los desarrolladores entiendan qué medidas deben tomar para que sus aplicaciones cumplan con las Políticas. Comuníquese con nosotros si [ve algún incumplimiento](#) o tiene alguna pregunta sobre [cómo administrar un incumplimiento](#).

Alcance de las políticas

Nuestras políticas de contenido se aplican a todo el contenido que aparece en las aplicaciones o al que se accede a través de ellas, lo que incluye los anuncios que se muestran a los usuarios y el contenido generado por el usuario que esté alojado en esas aplicaciones o al que se acceda a través de ellas. Además, se aplican a todo el contenido de la cuenta de desarrollador que se muestre públicamente en Google Play, lo que incluye el nombre del desarrollador y la página de destino del sitio web de desarrollador que se haya indicado.

No se permiten aplicaciones que permitan a los usuarios instalar otras aplicaciones en sus dispositivos. Las aplicaciones que brindan acceso a otras aplicaciones, juegos o software sin instalación, incluidas las funciones y experiencias proporcionadas por terceros, deben garantizar que todo el contenido al que brinden acceso cumpla con todas las [políticas de Google Play](#) y pueden estar sujetas a revisiones adicionales con respecto a las políticas.

Las definiciones de los términos que se usan en estas políticas tienen el mismo significado que en el [Acuerdo de Distribución para Desarrolladores](#) (DDA). Además de cumplir con estas políticas y el DDA, el contenido de las aplicaciones debe estar clasificado de acuerdo con nuestros [Lineamientos de clasificación del contenido](#).

Es posible que las aplicaciones inapropiadas para un público general o que generen una experiencia de mala calidad para los usuarios finales no sean aptas para participar de una promoción en Google Play. Sin embargo, esas aplicaciones permanecerán disponibles en Google Play siempre que cumplan con estas políticas y el DDA.

Google se reserva el derecho, a su total discreción, de incluir aplicaciones en Google Play o eliminarlas de dicha plataforma. Tomaremos medidas en función de diferentes factores; entre ellos, un patrón de comportamiento dañino o un riesgo alto de abuso. Para identificar el riesgo de abuso, utilizamos distintos elementos, como el historial de incumplimientos anteriores, los comentarios de los usuarios, el uso de marcas y personajes populares, y otros recursos.

Proceso de aplicación de las políticas

Si una aplicación incumple alguna de nuestras políticas, se la quitará de Google Play y se enviará una notificación por correo electrónico con el motivo específico de la eliminación. Los incumplimientos graves o repetidos (como software malicioso, fraude o aplicaciones que perjudiquen al dispositivo o al usuario) de estas políticas o del [Acuerdo de Distribución para Desarrolladores](#) (DDA) darán lugar a la rescisión de cuentas individuales o relacionadas.

Es posible que la eliminación o los avisos administrativos no indiquen cada uno de los incumplimientos presentes en la aplicación o en el catálogo amplio de aplicaciones. Los programadores son responsables de abordar los problemas de incumplimiento que se denuncien y de tomar cualquier medida adicional para garantizar que las aplicaciones cumplan, por completo, con las políticas. La falta de medidas con respecto a los incumplimientos de las políticas puede dar lugar a la imposición de otras acciones, lo que incluye la eliminación de la aplicación o la rescisión de la cuenta.

Cómo administrar y denunciar incumplimientos de políticas

Si tienes preguntas o inquietudes sobre la eliminación de una aplicación o los comentarios o calificaciones de los usuarios, puedes consultar los recursos que se incluyen a continuación o comunicarte con nosotros a través del [Centro de ayuda de Google Play](#). Sin embargo, no podemos brindarte asesoramiento legal. Si necesitas asesoramiento de este tipo, consulta a un asesor legal.

[Apelaciones y verificación de las aplicaciones](#)

[Cómo denunciar incumplimientos de políticas](#)

[Comunícate con Google Play para obtener detalles sobre la rescisión de una cuenta o la eliminación de una aplicación](#)

[Advertencias](#)

[Cómo denunciar aplicaciones y comentarios inapropiados](#)

[Se eliminó mi aplicación de Google Play](#)

[Información sobre la rescisión de cuentas de desarrollador de Google Play](#)

[Developer Distribution Agreement](#)